



MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDO DE OPERAÇÕES TERRESTRES

MANUAL DE CAMPANHA

SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

**1ª Edição
2025**



MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDO DE OPERAÇÕES TERRESTRES

MANUAL DE CAMPANHA
SEGURANÇA DAS INFORMAÇÕES
NAS OPERAÇÕES

1ª Edição
2025

PORTARIA – COTER/C Ex Nº 613, DE 21 DE OUTUBRO DE 2025

EB: 64322.016235/2025-20

Aprova o Manual de Campanha MC 2.50-1
Segurança das Informações nas Operações,
1ª edição, 2025.

O **COMANDANTE DE OPERAÇÕES TERRESTRES**, no uso da atribuição que lhe confere o inciso IV do artigo 28 das Instruções Gerais para o Sistema de Doutrina Militar Terrestre – SIDOMT (EB10-IG-01.005), 7ª edição, aprovadas pela Portaria do Comandante do Exército nº 2.451, de 9 de abril de 2025, resolve:

Art. 1º Aprovar o Manual de Campanha MC 2.50-1 Segurança das Informações nas Operações, 1ª edição, 2025, que com esta baixa.

Art. 2º Determinar que esta Portaria entre em vigor na data de sua publicação.

Gen Ex RICARDO AUGUSTO FERREIRA COSTA NEVES
Comandante de Operações Terrestres

(Publicado no Boletim do Exército nº 46, de 14 de novembro de 2025)

FOLHA REGISTRO DE MODIFICAÇÕES (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

SUMÁRIO

Pag

CAPÍTULO I - INTRODUÇÃO

1.1 Finalidades	1-1
1.2 Considerações Iniciais	1-2
1.3 Segurança das Informações nas Operações	1-4

CAPÍTULO II - SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

2.1 Considerações Iniciais	2-1
2.2 Dado	2-1
2.3 Informação	2-2
2.4 Ambiente Operacional	2-2
2.5 Informações no Ambiente Operacional	2-5
2.6 A Segurança das Informações	2-8
2.7 Gerenciamento de Risco	2-9

CAPÍTULO III - IDENTIFICAÇÃO DAS INFORMAÇÕES CRÍTICAS

3.1 Considerações Gerais	3-1
3.2 Visão Geral das Informações nas Operações	3-2
3.3 Informações Críticas para a Ameaça	3-4
3.4 Preparação para as Operações Militares	3-5

CAPÍTULO IV - ANÁLISE DAS AMEAÇAS

4.1 Considerações Gerais	4-1
4.2 Atores Empregados pela Ameaça	4-2
4.3 Motivações da Ameaça	4-3
4.4 Capacidades da Inteligência da Ameaça	4-4

CAPÍTULO V - ANÁLISE DAS VULNERABILIDADES

5.1 Considerações Gerais	5-1
5.2 Vulnerabilidades na Segurança da Informação no Pessoal	5-2
5.3 Vulnerabilidades na Segurança da Informação no Material	5-3
5.4 Vulnerabilidades na Segurança da Informação na Documentação	5-3
5.5 Vulnerabilidades da Segurança da Informação nas Áreas e Instalações ..	5-4
5.6 Vulnerabilidades na Segurança da Informação nos Meios de Tecnologia da Informação e Comunicações (MTIC)	5-4

CAPÍTULO VI - AVALIAÇÃO DOS RISCOS NA SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

6.1 Visão Geral	6-1
6.2 Avaliação de Probabilidade	6-1
6.3 Avaliação de Impacto	6-4
6.4 Nível do Risco	6-6
6.5 Classificação do Risco	6-7

CAPÍTULO VII - PLANEJAMENTO DA SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

7.1 Considerações Gerais	7-1
7.2 O Planejamento da Segurança das Informações nas Operações	7-3
7.3 Desmobilização das Operações Militares.....	7-4

ANEXO A - MODELO DE EXAME DE SITUAÇÃO DE SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

ANEXO B - MODELO DE PLANO DE SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES (PSIOp)

REFERÊNCIAS

CAPÍTULO I

INTRODUÇÃO

1.1 FINALIDADES

1.1.1 Este Manual de Campanha (MC) tem por finalidade orientar os Estados-Maiores (EM) dos diversos escalões da Força Terrestre (F Ter), bem como as estruturas de obtenção de dados e produção do conhecimento no planeamento e emprego da Segurança das Informações nas Operações (Seg Info Op).

1.1.2 Este manual de Seg Info Op contém 7 (sete) capítulos (Cap), cujas sínteses são apresentadas a seguir.

1.1.3 O Cap I traz as finalidades do manual, seu alcance e como ele foi concebido, destacando os fundamentos e as etapas do Processo de Segurança das Informações nas Operações (PSIOp). Serão abordados os conceitos de informação operacional, bem como da segurança dessas informações, seus objetivos e efeitos para as Forças Amigas (F Ami).

1.1.4 O manual foi elaborado com base no PSIOp. O Cap II – “Segurança das Informações nas Operações” aborda fundamentos doutrinários. Os demais capítulos correspondem a cada fase desse processo, a saber: Cap III – “Identificação das Informações Críticas”; Cap IV – “Análise das Ameaças”; Cap V – “Análise das Vulnerabilidades”; Cap VI – “Avaliação dos Riscos na Segurança das Informações nas Operações”; e Cap VII – “Planejamento da Segurança das Informações nas Operações”.

1.1.5 O Cap II descreve os fundamentos doutrinários da Seg Info Op, evidenciando suas capacidades, possibilidades e alcances. Serão apresentados: o que é dado e informação; caracterização de ambiente operacional; e as informações importantes para as operações. Por fim, a segurança das informações e o respectivo gerenciamento de risco serão contextualizados.

1.1.6 O Cap III apresenta uma visão geral das informações nas operações e detalha o que vem a ser Informações Críticas (IC), sua importância e riscos para as operações. Para melhor entendimento e visualização, serão citados alguns exemplos de IC.

1.1.7 O Cap IV é dedicado à análise das ameaças, desde a definição de possíveis atores, suas motivações e interesses, sua estrutura e capacidades da

Inteligência Militar (IM) da ameaça, abordando seus métodos de obtenção e emprego.

1.1.8 O Cap V traz a metodologia de análise das vulnerabilidades que possam surgir para as F Ami, em todos os subgrupos de medidas da Seg Info.

1.1.9 No Cap VI, será apresentada a técnica de avaliação de riscos, desde a avaliação da probabilidade e do impacto, passando pela qualificação do risco e sua classificação.

1.1.10 O Cap VII aborda o Planejamento da Segurança das Informações nas Operações (PSIOp). Nesse contexto, faz-se necessário ambientar quanto ao processo de emissão de Diretrizes de Seg Info Op e respectivos exames de situação e como se preparar para se contrapor às ameaças e à respectiva desmobilização das operações.

1.1.11 Ressalta-se que o gerenciamento de riscos da Seg Info Op será detalhado no PSIOp e trará um plano modelo, anexo a este manual.

1.2 CONSIDERAÇÕES INICIAIS

1.2.1 Esta publicação visa a focar a Seg de forma mais ampla, sendo essencial para garantir a proteção das F Ami, evitando que as ameaças obtenham a iniciativa, a superioridade de informações e a surpresa nas ações.

1.2.2 O processo de segurança das informações servirá como base para o manual, conforme a figura a seguir.

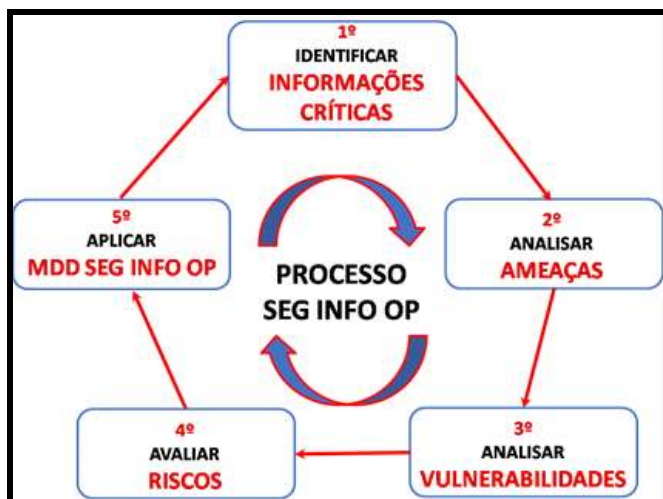


Fig 1-1 – Processo de Seg Info Op

1.2.3 O termo ameaça, constante no corpo deste manual, refere-se ao inimigo, à força adversa, à força oponente, etc. No Cap IV – “Análise da Ameaça”, não se pode confundir o termo ameaça (inimigo, oponente etc.) com a descrição de ameaça (ator com capacidade e motivado).

1.2.4 Inicialmente, cabe ressaltar que o MC 2.1 *Emprego da Inteligência* aborda as atividades e tarefas da Função de Combate de Inteligência (F Cmb Intlg), conforme segue:

- a) prover prontidão de Inteligência (Intlg);
- b) estabelecer a arquitetura de Intlg;
- c) obter dados e informações que alimentem o Processo de Integração Terreno, Condições Meteorológicas, Inimigo e Considerações Civas (PITCIC);
- d) gerar conhecimentos de Intlg;
- e) realizar ações de contrainteligência;
- f) coordenar as atividades do processo de Intlg;
- g) Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA);
- h) conduzir reconhecimentos especializados de Intlg;
- i) conduzir vigilância especializada de Intlg;
- j) coordenar a aquisição de alvos;
- k) prover apoio de Intlg às tarefas de informações; e
- l) proporcionar apoio de Intlg à busca continuada de ameaças.

1.2.5 Do exposto, pode-se inferir quais tarefas e atividades estarão diretamente ligadas à Seg Info Op, como nas alíneas “e”, “j” e “k”.

1.2.6 A Inteligência Militar (IM) desempenha um papel fundamental na transformação de informações em conhecimento útil para as operações militares. Ao coletar, analisar e interpretar dados, a Intlg fornece uma compreensão profunda do ambiente operacional, das intenções e capacidades do inimigo, das condições do terreno e das condições meteorológicas.

1.2.7 A análise do ambiente operacional é complexa e deve contemplar as seguintes perspectivas:

- a) dimensões interdependentes (física, humana e informacional);
- b) múltiplos domínios (terrestre, aéreo, marítimo, ciberespaço e espacial);
- c) expressões do poder (política, econômica, psicossocial, militar e científico-tecnológico); e
- d) níveis de planejamento e atuação (político, estratégico, operacional e tático).

1.2.8 A IM desdobra-se nos ramos Inteligência e Contrainteligência. Assim, a Seg Info Op está inserida no ramo Contrainteligência, que se divide nos segmentos da Segurança Orgânica (Seg Org) e Segurança Ativa (Seg Atv).

1.2.9 A delimitação do nome deste manual em “Segurança das Informações nas Operações” não implica uma menor abrangência das medidas de proteção. Pelo contrário, ao longo dos capítulos, será enfatizada a importância da

proteção das Info em Op, destacando sua prioridade para a F Ter. Essa escolha de título visa a refletir de maneira concisa o foco do manual, enquanto o conteúdo detalhado abordará as práticas e os protocolos essenciais para garantir a segurança da informação no contexto das operações militares.

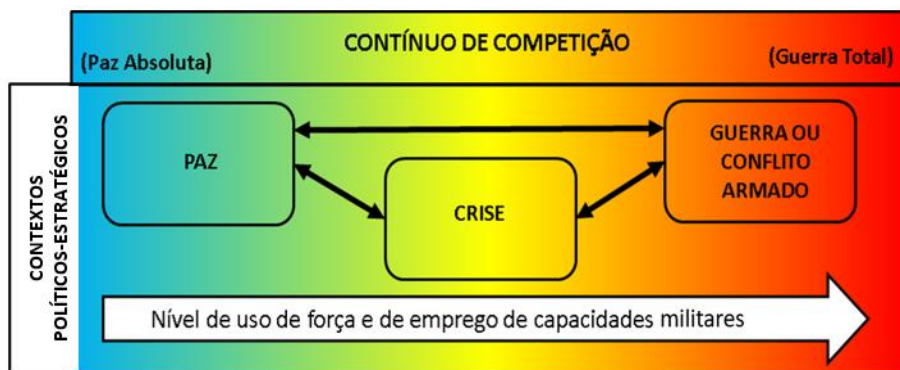


Fig 1-2 – Continuum da Competição

1.2.10 O Manual de Fundamentos *Contrainteligência* (MF 2.50) traz fundamentos essenciais para a segurança orgânica e ativa, embora não tenha como foco seu emprego nas operações militares.

1.3 SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

1.3.1 A Seg Info Op que será tratada neste manual está relacionada com a proteção da missão e dos combatentes, enfatizando a necessidade de proteger as informações operacionais sobre os movimentos e localização das tropas; detalhes da missão; unidades militares empregadas; imagens e sinais que possam comprometer o sigilo da missão, equipamentos etc.

1.3.2 A Seg Info, portanto, é um dos grupos de medidas da Seg Org e é composta pelos seguintes subgrupos de medidas:

- a) Segurança da Informação no Pessoal;
- b) Segurança da Informação na Documentação;
- c) Segurança da Informação no Material;
- d) Segurança da Informação nos Meios de Tecnologia da Informação e Comunicações; e
- e) Segurança da Informação nas Áreas e Instalações.

1.3.3 A Seg Info Op envolve uma série de medidas, passivas e ativas, em todas as fases da operação militar, desde o planejamento e preparação até a execução e pós-execução, em todo o espectro das ações militares e ambientes operacionais.

1.3.4 A Seg Info Op é um processo de identificação, análise e controle de IC sobre as F Ami que contenham Táticas, Técnicas e Procedimentos (TTP), capacidades, operações e outras atividades para:

- a) identificar ações que podem ser observadas por sistemas de inteligência da ameaça;
- b) determinar quais indicadores e sistemas podem obter e que possam ser interpretados ou combinados para obter IC a tempo de serem úteis para a ameaça; e
- c) selecionar e executar medidas que eliminem ou reduzam a um nível aceitável as vulnerabilidades das F Ami à exploração pela ameaça.

1.3.5 Importante ressaltar que as medidas de contrainteligência da Seg Org e da Seg Atv permanecerão em vigor em todo o contínuo de competição. Tal destaque visa a “ressaltar” que a Seg Info Op não irá focar os subgrupos de medidas que não a de Seg Info Op, pressupondo-se que as demais estarão em plena execução.

1.3.6 O tratamento das Info faz total diferença no ambiente operacional, seja para a vitória ou para a derrota no combate. Assim, a proteção dessas Info é essencial para o planejamento e a condução de operações militares e para a manutenção da legitimidade, legalidade e estabilidade do país. Como já citado, essas Info estão em todos os ambientes, tais como pessoal, profissional, familiar e necessitam ser protegidas das ameaças.

CAPÍTULO II

SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

2.1 CONSIDERAÇÕES INICIAIS

2.1.1 Este capítulo aborda os principais fundamentos e generalidades da Seg Info Op. Para melhor entendimento, serão abordados inicialmente o dado e a informação. O ambiente operacional e as informações nas operações serão descritos na sequência. Por fim, serão apresentados os fundamentos da Seg Info e do Gerenciamento dos Riscos em Operações (GRO).

2.2 DADO

2.2.1 O dado é a base da Info, representando qualquer sinal ou observação coletada do ambiente. No contexto das operações militares, os dados podem abranger uma ampla gama de elementos, sobre pessoas, material militar, condições do ambiente operacional, até de perfis e motivações de chefes de estado e comandantes militares. Os dados constituem a essência da informação, que, por meio de um processo analítico, adquirem significado e relevância, contribuindo para o processo de tomada de decisões.

2.2.2 O dado possui as seguintes características:

- a) assinatura – dado que torna algo identificável ou faz com que se destaque;
- b) associação – relação de um dado com outras informações ou atividades críticas;
- c) perfil – somatório das assinaturas e associações; e
- d) exposição – período que o dado foi observado.

2.2.3 As formas como os eventos são desencadeados e organizados são consideradas padrões. A ameaça procura padrões e assinaturas para estabelecer um perfil.

2.2.4 Quando são observadas diferenças entre o perfil padrão de uma atividade e suas ações mais recentes ou atuais, encontra-se um contraste, que possivelmente será avaliado pela ameaça.

2.2.5 É possível programar medidas que reduzam a visibilidade de dados.

2.2.6 Os dados são analisados de forma ampla, sejam eles abertos (disponíveis) ou fechados (protegidos). Eles poderão ser obtidos, reunidos e interpretados, gerando uma informação útil à ameaça.

2.3 INFORMAÇÃO

2.3.1 A informação é a base da Intlg, ou seja, o produto da obtenção, processamento, integração, avaliação, análise e interpretação de dados negados e disponíveis sobre forças ou elementos hostis ou potencialmente hostis, ou de áreas de operações reais ou potenciais.

2.3.2 As pessoas atribuem significado aos dados e usam essas informações para compreender, comunicar, tomar decisões e agir.

2.3.3 Os dados e as informações podem ser usados em qualquer nível de emprego. O indivíduo (combatente ou não combatente) que tiver acesso a esses ativos atribuirá valor e significado distintos, de acordo com seu nível de compreensão do ambiente operacional.

2.3.4 O significado da informação que leva à compreensão e à tomada de decisão depende tanto da própria informação (dados e seu contexto) quanto de fatores que influenciam a forma como um receptor interpreta essa informação.

2.3.5 O Oficial de Inteligência desempenha um papel importante na construção do conhecimento, pois sua capacitação e experiência são determinantes na interpretação e análise das informações disponíveis. Contudo, vários fatores podem influenciar esse processo analítico, incluindo atitude, preconceito, cognição, cultura, desejos, emoções, especialização, instinto e percepção.

2.3.6 Esses elementos podem afetar a objetividade e a precisão das conclusões, tornando essencial que o analista esteja consciente dessas influências para minimizar distorções e assegurar que o conhecimento produzido seja confiável e útil para a tomada de decisões.

2.3.7 O levantamento de quais informações são de interesse da ameaça constitui a primeira fase do PSIOp.

2.4 AMBIENTE OPERACIONAL

2.4.1 Nas Op Mil, as informações são disponibilizadas e gerenciadas em três principais dimensões do ambiente operacional: física, humana e informacional. Cada uma dessas dimensões tem características e métodos específicos para a obtenção e utilização de dados.

2.4.2 A concepção das operações terrestres prevê a manobra física e a manobra informacional.

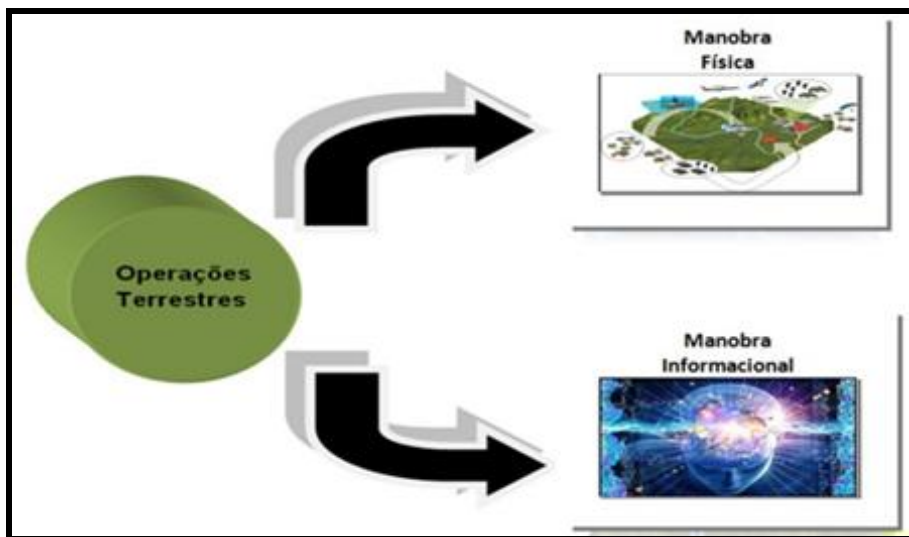


Fig 2-1 – Síntese das operações terrestres

2.4.3 Os fatores operacionais são aspectos militares e não militares que diferem de uma Área de Operações (A Op) para outra e afetam, significativamente, as operações. O conhecimento deles é fundamental para desenvolver um entendimento completo do ambiente operacional e se obter a consciência situacional.

2.4.4 No planejamento da Seg Info Op, compreender as três dimensões permite um planejamento mais preciso e adaptado às condições reais do ambiente operacional.



Fig 2-2 – Dimensões do ambiente operacional terrestre (DMT)

2.4.5 As Info Op estão distribuídas em todas as dimensões, de acordo com os aspectos gerais a seguir.

2.4.5.1 Dimensão Humana

2.4.5.1.1 Envolve a compreensão das populações locais, culturas, sistemas políticos e sociais, bem como as atitudes e comportamentos dos indivíduos e grupos. As informações nesta dimensão são obtidas por fontes e submetidas a técnicas de análise, como citado a seguir.

- a) Inteligência de Fontes Humanas (HUMINT) e tropa como sensor – coletada por meio de entrevistas, informantes e observação direta para obter informações sobre atividades, atitudes da população e possíveis ameaças.
- b) Análise sociocultural – estudos e análises das culturas locais, línguas, religiões e estruturas sociais para melhor interação e operação no ambiente humano.
- c) Análise da geografia humana – estuda e analisa a interação do homem com o espaço físico que habita quanto aos aspectos demográficos, sociais, econômicos e culturais.

2.4.5.2 Dimensão Física

2.4.5.2.1 Abrange o terreno, as condições meteorológicas, a infraestrutura e os recursos físicos presentes no campo de batalha. As informações nesta dimensão são obtidas por fontes e submetidas a técnicas de análise, conforme a seguir.

- a) Sensores e sistemas de reconhecimento – drones, satélites, radares e sensores terrestres coletam dados sobre o terreno, clima e movimentação de tropas e veículos.
- b) Mapas e Sistemas de Informação Geográfica (GIS) – fornecem representações detalhadas do terreno e da infraestrutura e localização de unidades e recursos.
- c) Relatórios meteorológicos – informações sobre condições climáticas que podem afetar a visibilidade, a mobilidade e a eficácia das operações.
- d) PITCIC – analisa o ambiente operacional, o terreno e as condições meteorológicas.

2.4.5.3 Dimensão Informacional

2.4.5.3.1 Compreende a obtenção, o processamento, a proteção e a disseminação de informações, tanto amigas quanto inimigas. As informações nesta dimensão são obtidas por fontes e submetidas a técnicas de análise, como citado a seguir.

- a) Fontes Humanas (HUMINT) – obtenção de dados e informações de forma direta junto à população, com bom nível de credibilidade e confiabilidade.
- b) Inteligência de Sinais (SIGINT) – interceptação e análise de comunicações, incluindo rádio, telefones e comunicações eletrônicas.

- c) Cibernética (Ciber) – proteção de sistemas de informação militar e ataque a sistemas de informação para coletar dados ou interromper operações.
- d) Análise de Geointeligência (GEOINT) – analisa de forma integrada as imagens, as informações geográficas e a atividade de inteligência de imagens.
- e) Operações Psicológicas (Op Psc) – utilizam informações para influenciar as atitudes e comportamentos de grupos-alvo.

2.4.6 O escopo do planejamento da Seg Info Op deve determinar os dados que os sistemas de inteligência da ameaça podem obter e ser interpretados ou combinados para obter IC.

2.4.7 As informações levantadas precisam ser protegidas por meio de medidas preventivas e ativas que eliminem ou reduzam, a um nível aceitável, as suas vulnerabilidades à exploração pela ameaça.

2.4.8 A integração das informações disponíveis nas dimensões é essencial para a eficácia das operações militares. Por exemplo, informações físicas sobre o terreno (dimensão física) são combinadas com dados de inteligência humana sobre a população local (dimensão humana) e comunicações interceptadas (dimensão informacional) para criar um quadro situacional o mais completo e preciso possível.

2.4.9 As tecnologias modernas, como Inteligência Artificial (IA) e *big data*, ajudam a processar e a integrar essas vastas quantidades de informações, permitindo a tomada de decisão mais rápida e eficaz. Nesse cenário, é fundamental a proteção dos ativos de informação de forma a negar à ameaça sua exploração.

2.4.10 Para a tomada de decisão, as informações integradas fornecem aos comandantes uma visão mais ampla, permitindo decisões informadas e oportunas. A segurança desses ativos é essencial para a preservação do processo decisório.

2.4.11 Essas práticas visam assegurar a “liberdade de ação” às forças militares em operar com a máxima eficácia e segurança, respondendo rapidamente a ameaças e aproveitando oportunidades no ambiente operacional complexo.

2.5 INFORMAÇÕES NO AMBIENTE OPERACIONAL

2.5.1 Caracterizar o que vem a ser as Info no ambiente operacional, visto ser essencial para entender “o quê” deve ser protegido.

2.5.2 Na figura a seguir, é possível identificar grupos de atores e fatores que detêm informações relevantes para as operações militares, nas suas respectivas dimensões do combate, que serão analisadas visando à Seg Info Op.

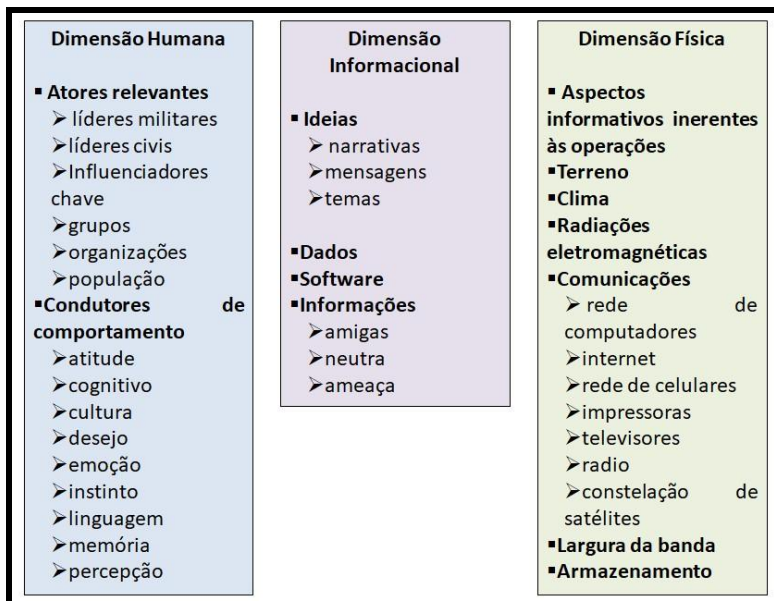


Fig 2-3 – Considerações informacionais

2.5.3 O ambiente das informações é composto por fatores sociais, culturais, linguísticos, psicológicos, técnicos e físicos que afetam como os humanos e os sistemas automatizados obtêm e geram conhecimentos, agem e são impactados pela informação.

2.5.4 A informação nas operações pode ser gerada e/ou transmitida por qualquer dos meios e atores citados na Fig 5. Tais informações estão muito além de dados e conhecimentos sobre o desdobramento operacional das tropas militares e ações militares.

2.5.5 Todas as informações das dimensões humana, informacional e física devem ser avaliadas e protegidas, de acordo com a sua sensibilidade, criticidade e risco. Essas informações, de posse da ameaça, poderão desequilibrar o poder de combate militar.

2.5.6 A informação, como dinâmica do poder de combate, é explorada por meio das seguintes atividades: habilitar, proteger, informar, influenciar e atacar. Este manual abordará a proteção das informações em operações.

2.5.7 A obtenção da vantagem da informação em operações é consolidada quando uma força detém a iniciativa em termos de compreensão situacional, tomada de decisão e comportamento relevante dos atores. A figura a seguir retrata as atividades da informação, os objetivos e os princípios da vantagem informacional.

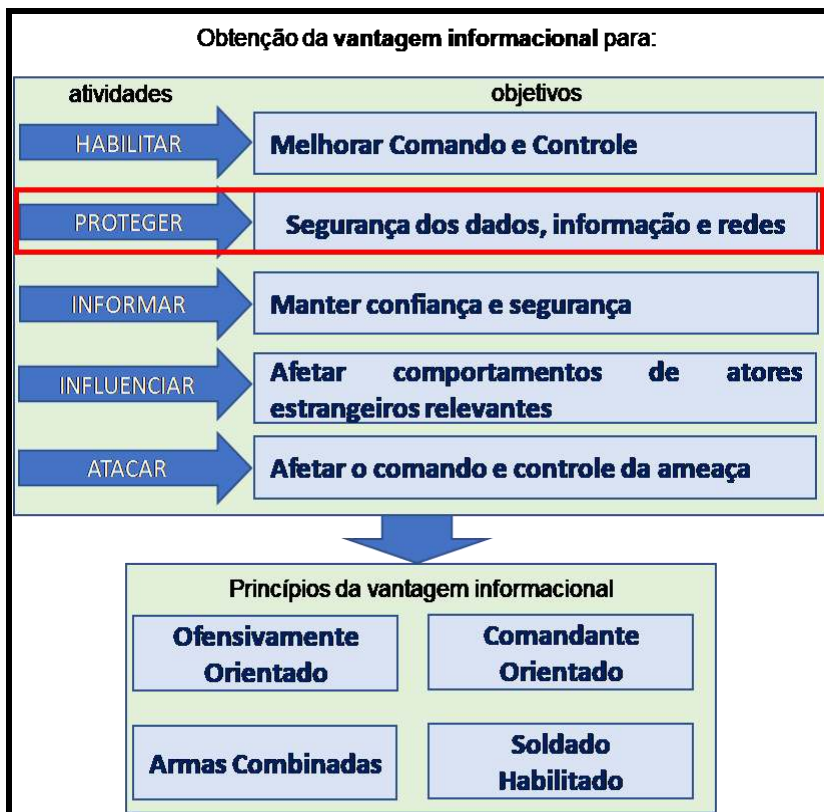


Fig 2-4 – Estrutura da vantagem informacional

2.5.8 A Seg Inf Op tem exclusivamente a função de proteger as informações durante os conflitos armados, com o objetivo de proteger dados, informações e redes/meios de transmissão.

2.5.9 O oponente irá realizar seu Exame de Situação do Inimigo (Exm Sit Ini), no caso das F Ami, e realizará processos semelhantes ao PITCIC.

2.5.10 O MC *Processo de Integração Terreno, Condições Meteorológicas, Inimigo e Considerações Civas (PITCIC)* consiste em quatro fases: definição do ambiente operacional; identificação dos efeitos do ambiente sobre as operações; avaliação da ameaça; e determinação das possíveis Linhas de Ação (L Aç) da ameaça.

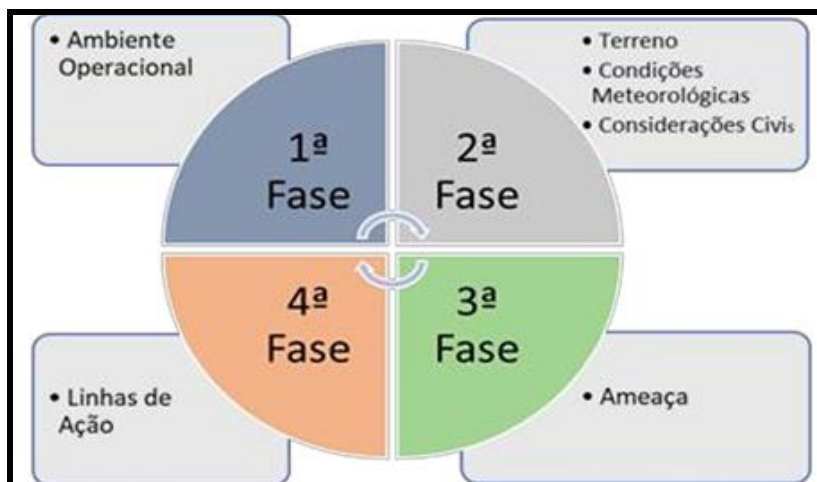


Fig 2-5 – Fases do PITCIC

2.6 A SEGURANÇA DAS INFORMAÇÕES

2.6.1 O emprego da Seg Info Op exerce sua função de proteção, negando aos adversários informações ligadas às operações militares sobre recursos, atividades, limitações e intenções amigas que os adversários necessitam e possam usar para tomar decisões operacionais mais assertivas.

2.6.2 A Seg Info tem como princípios a confidencialidade, a integridade, a disponibilidade, a autenticidade, a inviolabilidade e a irretratabilidade, conforme definidos no MC *Contraineligência*.

2.6.3 O comandante de uma operação deve ter à sua disposição recursos necessários para reduzir ou eliminar os riscos, além de ter liberdade de ação para implantar as medidas que julgar necessárias para o tratamento do risco. Os comandantes, em todos os níveis, devem garantir a segurança das informações em todas as fases da operação.

2.6.4 A Seg Info Op consiste no Gerenciamento do Risco e do Plano de Segurança das Informações nas Operações (PSIOp).

2.6.5 O risco operacional é qualquer fato, ato ou condição, seja potencial ou não, que possa gerar probabilidade de ocorrência de impactos nos objetivos estabelecidos, criando insegurança nas ações durante o conflito armado.

2.6.6 O Gerenciamento do Risco Operacional (GRO) propicia ao decisor identificar e tratar os riscos inerentes a uma operação militar. Devem ser considerados os riscos de menor impacto, como avaria de material, e os de alto impacto, como perda de vida humana ou comprometimento da missão.

2.6.7 Gerenciar riscos é fator decisivo para o sucesso de uma operação militar, e a Seg Info Op é parte direta do gerenciamento desses riscos.

2.6.8 O Processo de Gerenciamento de Risco para a Seg Info Op é sistemático e deve ser usado para identificar, controlar e proteger as informações que podem ser exploradas pela ameaça.

2.6.9 Tal processo prevê a definição de medidas que mitiguem ou evitem a exploração ou a exposição do dado pela ameaça. Da mesma forma, busca preservar a ação de comando ao permitir opções de tratamento do risco identificado.

2.6.10 O Plano de Gerenciamento de Risco (PGR) da Seg Info Op, ao ser bem empregado, auxilia na aplicação do poder militar, cabendo ao comandante incorporá-lo às operações.

2.6.11 Esse processo deve ser contínuo e integrado em todas as operações e atividades militares. Todos são responsáveis pela manutenção da segurança. O principal ativo a ser protegido é a informação em todo espectro dos conflitos.

2.7 GERENCIAMENTO DE RISCO

2.7.1 Gerenciamento de Risco da Seg Info Op é uma ferramenta que o comandante possui para avaliar os riscos operacionais ligados à informação e o quanto desses riscos está-se disposto a aceitar em circunstâncias específicas, assim como é feito no GRO.

2.7.2 O gerenciamento do risco e seu processo não estão direcionados à proteção completa de ativos envolvidos na operação, mas sim às informações operacionais críticas. Isso pode acarretar um desvio de prioridade voltada aos objetivos operacionais estabelecidos.

2.7.3 O Processo de Gerenciamento de Risco é contínuo e cíclico, devendo ocorrer durante todas as fases do conflito. Deve ser considerada a natureza mutável das informações da própria ameaça e das avaliações das vulnerabilidades em toda a operação.

CAPÍTULO III

IDENTIFICAÇÃO DAS INFORMAÇÕES CRÍTICAS

3.1 CONSIDERAÇÕES GERAIS

3.1.1 O presente capítulo refere-se à 1ª Fase do Processo de Segurança das Informações nas Operações, a qual visa a identificar quais informações devem ser protegidas pelas F Ami. Essa fase é a base para a preparação da Seg Info Op.

3.1.2 Os ativos para a Seg Info Op são todos os recursos ou elementos que possuem valor para a F Ter em termos de informação e que precisam ser protegidos para garantir sua integridade, confidencialidade e disponibilidade.

3.1.3 As IC são dados específicos das F Ami sobre as capacidades operacionais, dados de Intlg, ativos de tecnologia, doutrina, materiais, planos operacionais, localização de tropas etc. cuja proteção é vital para o cumprimento da missão.

3.1.4 A obtenção de IC pelo oponente tem o objetivo de obter vantagem militar, política, diplomática, econômica ou tecnológica. Nota-se que informações que são críticas em uma fase da missão podem não ser críticas nas fases subsequentes.

3.1.5 As IC incluem dados e informações que, individualmente ou em conjunto, revelam detalhes importantes sobre as atividades amigas e, portanto, exigem um nível de proteção contra a inteligência da ameaça. As IC têm como alvo os ativos mais relevantes para as operações militares.

3.1.6 O tópico anterior, em síntese, define que as IC a serem identificadas, analisadas, avaliadas e aplicadas nas medidas de Seg Info Op devem ter ligação direta com o combate, com o ambiente operacional.

3.1.7 Após levantamento e avaliação das ameaças, a estrutura de Intlg deve realizar um estudo sobre o sistema de Intlg da ameaça, levantando suas capacidades de obtenção de dados, disciplinas de Intlg disponíveis, níveis de conhecimento, tecnologia, equipamentos e doutrina, e, da mesma forma, sua estrutura para as operações e perfil de emprego.

3.1.8 O PITCIC consiste em um processo cíclico de análise do ambiente operacional e das ameaças, conduzido pelo Oficial de Inteligência e apoiado pela Célula de Inteligência que busca disponibilizar os conhecimentos necessários para o Processo de Planejamento e Condução das Operações

Terrestres (PPCOT, ciclo das operações) e orienta os esforços dos meios de obtenção de dados.

3.1.9 Tal esforço visa, sobretudo, a proteger as ações das F Ami desde o tempo de preparação para o conflito armado até o pós-guerra. Além disso, busca proteger o emprego da Intlq, em todos os níveis, das fases do Ciclo de Inteligência e das operações militares.

3.1.10 Ao mesmo tempo em que os dados amigos são protegidos, eles são negados à ameaça, impedindo ou dificultando a ação desta, a sua obtenção da surpresa, o ineditismo e a vantagem no combate.

3.1.11 A eficácia da Seg Info depende essencialmente do conhecimento profundo das ameaças, incluindo suas capacidades e fraquezas. É prudente assumir, inicialmente, que a atividade de inteligência do oponente seja, no mínimo, tão eficiente quanto a da F Ami.

3.1.12 Esse entendimento sublinha a necessidade de constante vigilância e aprimoramento das medidas de segurança, garantindo que a proteção da informação esteja sempre um passo à frente das possíveis ameaças.

3.1.13 Para o sucesso das operações militares, a surpresa é um princípio essencial. Ela depende dos conhecimentos disponíveis, da rapidez dos movimentos executados e da efetividade da Seg Info, tanto ao negar conhecimentos às ameaças quanto ao detectar e neutralizar as atividades de degradação dos meios e sistemas das F Ami ligados às informações nas operações.

3.2 VISÃO GERAL DAS INFORMAÇÕES NAS OPERAÇÕES

3.2.1 As informações apresentam-se nas operações militares de várias formas, utilizando uma combinação de tecnologias e processos específicos. Aqui estão alguns dos principais ativos e suas informações que são alvos de ações de obtenção pelas ameaças:

- a) sensores e sistemas de obtenção de dados – radares, câmeras de vigilância, drones e sistemas de reconhecimento óptico e infravermelho para coletar informações sobre o ambiente operacional;
- b) redes de comunicação – utilizadas para transmitir informações entre unidades militares, com segurança e em tempo real. Isso inclui sistemas de rádio, satélite e redes de comunicação por fibra ótica;
- c) ferramentas de IA e análise de dados – empregadas para processar grandes volumes de dados coletados, identificar padrões e fornecer análises preditivas que auxiliam na tomada de decisões;

- d) Sistemas de Informação Geoespacial (GIS) – permitem a análise e a visualização de informações geográficas, como mapas digitais atualizados, pontos de interesse e rotas estratégicas;
- e) Centros de Comando e Controle (CC²) – locais onde as informações são centralizadas, permitindo que comandantes e líderes militares tenham uma visão ampliada do campo de batalha e das operações em andamento;
- f) criptografia e segurança da informação – para proteger as comunicações e dados sensíveis contra interceptação e ataques cibernéticos; e
- g) fontes de dados – dados de fontes diversas, incluindo Inteligência Humana (HUMINT), Inteligência de Sinais (SIGINT), Inteligência de Saúde (MEDINT), Inteligência Cibernética (CIBERINT), Geointeligência (GEOINT), Inteligência de Fontes Abertas (OSINT), Inteligência de Assinatura de Alvos (MASINT), Inteligência Técnica (TECHINT).

3.2.2 Informações de possíveis alvos de alto valor, como depósito de munições, bases logísticas, radares, centros de comandos, etc., são exemplos de objetivos da inteligência da ameaça.

3.2.3 Essas informações podem ser obtidas por meios cibernéticos, *hackeando* e rastreando telefones celulares ou mesmo invadindo redes de comando militar, por meio de operações de inteligência de sinais mais tradicionais (como a triangulação da localização de radares e rádios), via reconhecimento por satélite ou por observadores e drones na linha de frente das tropas.

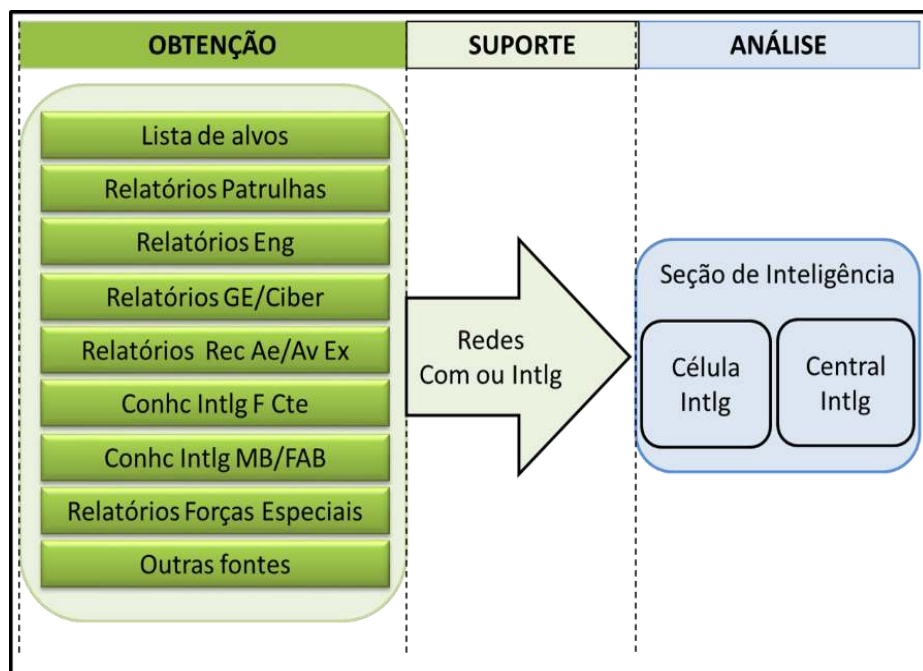


Fig 3-1 – Fluxo dos dados obtidos

3.3 INFORMAÇÕES CRÍTICAS PARA A AMEAÇA

3.3.1 Os dados e os conhecimentos sobre os objetivos operacionais das F Ami sempre serão importantes para a ameaça em qualquer tipo de conflito.

3.3.2 De acordo com o escalão e a missão, as necessidades de conhecimento da ameaça poderão abranger, além de aspectos militares, outros relacionados a aspectos fisiográficos, históricos, etnológicos, políticos, econômicos, científico-tecnológicos e psicossociais.

3.3.3 As ameaças podem ter como alvo das nossas forças: centros e nós de C², sensores de vigilância e aquisição de alvos, sistemas e infraestrutura de telecomunicações e redes, *links* de informação, como receptores de radiofrequência, radares, dispositivos de comunicação e protocolos de informação. Trata-se de alvos de ameaças que degradam as comunicações, a navegação e o controle de fogo.

3.3.4 A prioridade de obtenção de informações pela ameaça varia de acordo com a situação, a natureza do escalão considerado e dos conhecimentos disponíveis.

3.3.5 As IC para a ameaça podem ser traduzidas como sendo as suas Necessidades de Inteligência (NI), que, de maneira semelhante à doutrina das F Ami, são satisfeitas pelos conhecimentos que elas precisam ter à sua disposição, relativos ao terreno, inimigo, condições climáticas e meteorológicas, a fim de poder cumprir a missão com êxito.

3.3.6 Para atender ao PSIOp das F Ami, as NI da ameaça devem ser relacionadas às suas capacidades. O acrônimo DOAMEPI (Doutrina, Organização e/ou Processos, Adestramento, Material, Educação, Pessoal e Infraestrutura) pode ser usado para levantar as capacidades operacionais da ameaça.

3.3.7 Das informações possíveis de serem levantadas pelos oponentes, aquelas que permitem o levantamento das possibilidades das F Ami são as mais importantes para a Seg Info proteger.

3.3.8 No nível tático, podem ser consideradas IC as seguintes informações das tropas amigas:

- a) ordem de batalha – informações sobre o dispositivo, composição, valor, atividades recentes e atuais e peculiaridades;
- b) pessoal – efetivo pronto, efetivo baixado, lideranças e situação da moral de tropa;
- c) possibilidades – capacidades da tropa no ambiente operacional em razão dos seus meios e pessoal;

- d) situação logística – situação de disponibilidade e perdas de Material de Emprego Militar (MEM) das diversas classes;
- e) planos operacionais e logísticos – quais os planos em vigor e medidas de proteção;
- f) vulnerabilidades – deficiências que podem ser exploradas em relação à segurança das informações do pessoal, os Meios de Tecnologia da Informação e Comunicações (MTIC), material, informações, áreas e instalações;
- g) dados pessoais – dados biográficos, perfil dos comandantes e personalidade do decisor;
- h) Inteligência Artificial (IA) – sistemas empregados, prioridades de coleta e análise, centros de IA das F Ami, formas de difusão e capacidades;
- i) medidas de segurança orgânica em execução – rotinas de rotas logísticas ou operacionais, sistemas de reconhecimento de permissão de acesso; medidas de segurança em posto de comando e central Intlg etc.;
- j) capacidades de interceptação – de mísseis e foguetes, emissões eletromagnéticas, radares, de ARP (drones), ações ciber;
- k) estrutura e funcionamento da Intlg – capacidades e limitações existentes em todas as disciplinas de Intlg, particularmente de fontes humanas e tecnológicas;
- l) relacionamento da tropa com a população – legitimidade e apoio da população, possibilidade de colaborar com a ameaça, repasse de informações do ambiente operacional;
- m) normas e medidas de segurança em vigor – levantar o nível de segurança adotado no ambiente operacional;
- n) capacidade de realizar segurança ativa – contraterrorismo, contra ações psicológicas, contrassabotagem, contraespionagem e contrainteligência interna; e
- o) outras IC não discriminadas neste capítulo que venham a ser úteis de acordo com as fases da operação.

3.3.9 Cabe ressaltar que este manual não visa a listar todas as possíveis IC para cada tipo de operação, mas sim possibilitar o entendimento dos fundamentos e a aplicabilidade das informações visando à confecção e ao emprego do Plano de Seg Info Op. As particularidades de cada tipo de operação e seus respectivos NI e ONI serão levantadas durante o Exm Sit Ini.

3.4 PREPARAÇÃO PARA AS OPERAÇÕES MILITARES

3.4.1 A fase de preparação para a Seg Info Op consiste no levantamento inicial das IC amigas de interesse da Intlg da ameaça.

3.4.2 As IC de posse da ameaça podem ter como consequências diretas: emprego de poder militar contra as forças amigas e perda de poder de combate amigo.

3.4.3 Quanto mais informações sobre o “inimigo” uma força tiver, maior será a eficiência no planejamento e condução de suas operações militares.

3.4.4 A preparação da segurança das informações tem o propósito de identificar a informação crítica, bem como determinar e priorizar as possibilidades da inteligência da ameaça e seus impactos nas L AÇ amigas.

3.4.5 O produto final é a Lista de Informações Críticas (LIC) que será utilizada no PSIOP e no consequente Plano de Gerenciamento de Risco Operacional (PGRO). Essa etapa é uma das mais difíceis do processo e a mais importante a ser realizada. Não se pode proteger tudo, logo as IC devem ser avaliadas e priorizadas.

INFORMAÇÃO CRÍTICA (para a Ameaça)	PRIORIDADE (estimado pelo EM da F Ami)	ORIGEM DA INFORMAÇÃO (nas F Ami)	IMPACTO VISUALIZADO (estimado pelo EM da F Ami)
QUANTITATIVO DE MUNIÇÃO DA BATERIA ASTROS	1	- RECURSOS HUMANOS - SISTEMAS DE C ² - ANEXO LOGÍSTICO DA FTC	PERDA DE PODER DE COMBATE
LOC DA Z REU DA TROPA BLINDADA	2	- ORDEM DE OPERAÇÕES - SISTEMAS DE C ² - RECURSOS HUMANOS	PERDA DE C ² E DO FATOR SURPRESA

Quadro 3-1 – Exemplo da Lista de Informações Críticas (LIC)

3.4.6 O fluxograma a seguir destaca a Metodologia a ser aplicada desde o levantamento das Info Op até a caracterização do RISCO, que será avaliado e classificado para que as medidas para evitar, mitigar ou eliminar sejam aplicadas.

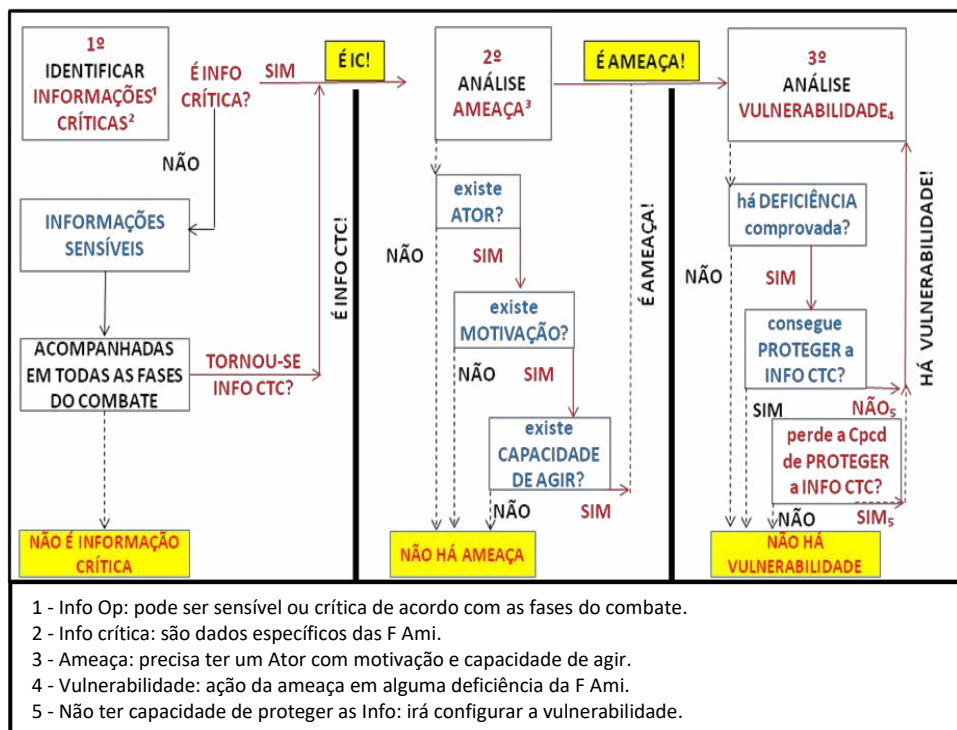


Fig 3-2 – Fluxograma do Processo de Segurança das Informações nas Operações (PSIOp)

3.4.7 As fases seguintes, “4ª Fase – Avaliar Riscos” e “5ª Fase – Aplicar Medidas de Segurança das Informações nas Operações”, serão abordadas nos capítulos VI e VII, respectivamente.

CAPÍTULO IV

ANÁLISE DAS AMEAÇAS

4.1 CONSIDERAÇÕES GERAIS

4.1.1 O presente capítulo refere-se à 2ª fase do PSIOp, que visa a analisar as possíveis ameaças às F Ami no ambiente operacional.

4.1.2 As diretrizes de Seg Info quanto à avaliação das ameaças serão difundidas pela cadeia de comando para a difusão junto às tropas em operações e cumprimento das ordens.

4.1.3 A ameaça compreende a conjunção de ator, motivação e capacidade de realizar ação hostil, real ou potencial. Deve ter, ainda, possibilidade de, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e seus valores, bem como as áreas e instalações, podendo causar danos a uma operação militar, particularmente, à segurança das informações.

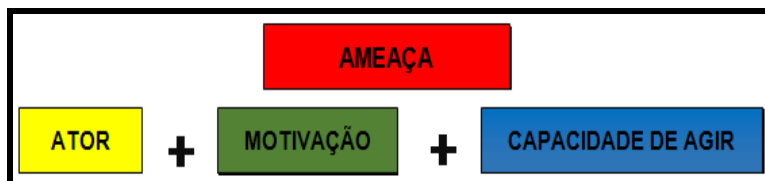


Fig 4-1 – Síntese do conceito de ameaça

4.1.4 Uma ameaça pode ser um adversário ou inimigo. O adversário é reconhecido como potencialmente hostil e contra o qual o uso da força pode ser considerado. O inimigo é a parte identificada como hostil, contra a qual é autorizado o uso da força.

4.1.5 Para constituir-se em AMEAÇA, é necessário que seja identificado e qualificado o ATOR que agirá contra as F Ami, como também se há MOTIVAÇÃO e em qual grau que o faça se expor e empregar meios, pessoal e material, caracterizando sua CAPACIDADE DE AGIR. Os componentes da ameaça quanto mais integrados, em tese, mais “fácil” será sua identificação e vice-versa.

4.1.6 A caracterização da ameaça é essencial para o planejamento e, ao mesmo tempo, muito difícil e complexa, não se tratando somente da Intlg adversa.

4.1.7 O ambiente operacional e as ações militares são condicionados pelos seguintes aspectos:

- a) hiperconectividade;
- b) urbanização;
- c) relevância da dimensão informacional;
- d) judicialização do combate;
- e) automação ampliada;
- f) aceleração do combate;
- g) maior letalidade seletiva e monitoramento das ações; e
- h) extrapolação.

4.1.8 Há que se destacar os aspectos da urbanização, relevância da dimensão informacional e extrapolação do combate para entender a motivação que a ameaça terá durante sua fase de obtenção das informações operacionais.

4.1.9 A urbanização das operações é uma tendência dos conflitos modernos, nos quais os objetivos militares incidirão sobre grandes áreas urbanas, recursos estratégicos e cadeias logísticas. Assim, os objetivos táticos podem transcender a efeitos estratégicos, além do Teatro de Operações (TO).

4.1.10 A relevância da informação (dimensão informacional) é inequívoca nas operações, tão importante quanto o efeito letal. O campo das informações é passível de ser explorado e potencializado nos níveis político e estratégico. Nesse aspecto, é enfocada a importância da manutenção da legitimidade, o apoio da população, por meio da narrativa do conflito e das percepções, em todas as fases do conflito armado.

4.1.11 A extrapolação prevê que a guerra não está confinada dentro do espaço de batalha, ou seja, as informações que serão buscadas pela ameaça seguirão a mesma premissa.

4.2 ATORES EMPREGADOS PELA AMEAÇA

4.2.1 Em linhas gerais, a ameaça pode empregar atores de diversas naturezas e capacidades para obter informações das F Ami, normalmente, em ações não cinéticas.

4.2.2 O emprego da Intlg naturalmente será o condutor dessas ações, o qual empregará todos os meios possíveis de obtenção de dados.

4.2.3 As ameaças podem abranger uma ampla gama de atores, incluindo indivíduos, grupos organizados, forças paramilitares ou militares, elementos criminosos, estados-nações ou alianças nacionais. Cada um desses atores possui capacidades e motivações distintas, o que exige uma abordagem

diversificada e adaptativa para identificar, avaliar e neutralizar os riscos que representam.

4.2.4 Entre possíveis atores que podem vir a impactar a segurança da informação, encontram-se os combatentes e os não combatentes. Estes últimos podem abranger população local, autoridades, integrantes de grupos criminosos, mídia em geral etc.

4.2.5 Ações cinéticas podem ser realizadas em apoio às ações da Intlg no contexto da Seg Info Op.

4.2.6 Esses atores atuarão no ambiente operacional contemporâneo, em todas as dimensões e nos múltiplos domínios do combate. Assim, a análise da ameaça deve abranger todas as expressões do poder nacional para apoiar ao planejamento das operações.

4.2.7 Coerente com a definição do aspecto extrapolação, serão citadas algumas ações no espaço de batalha para obter dados ou intervir na dimensão informacional:

- a) publicações de ativistas digitais e influenciadores;
- b) tentativas de intrusão e ataques cibernéticos;
- c) campanhas de desinformação;
- d) eventos no domínio espacial, intervenção no uso de satélites de comunicação;
- e) emprego de mísseis de longo alcance para fins militares;
- f) plataformas de lançamentos de mísseis fora do TO; e
- g) pilotos em estações remotas fora do TO.

4.3 MOTIVAÇÕES DA AMEAÇA

4.3.1 As motivações da ameaça sobrepõem os objetivos operacionais de conquista de espaços físicos, centros urbanos etc. Dependendo do Estado Final Desejado estabelecido pelo Comandante da Operação e pelo Chefe de Estado, as motivações para a força oponente serão as mais diversas possíveis.

4.3.2 Dito isso, pode-se inferir que as motivações surgirão de demandas operacionais, políticas ou de qualquer expressão do poder nacional. Assim, a motivação vai induzir ou ditar quais meios e atores serão empregados para a obtenção das informações (NI e EEI) planejadas.

4.3.3 O emprego da Intlg é inequívoco para o planejamento e a condução do processo de obtenção dos dados, embora os atores nem sempre sejam militares, especializados em Intlg ou não.

4.3.4 Da mesma forma, pode-se afirmar que ações em diversas áreas também ocorrerão simultaneamente, particularmente nos campos político e econômico do poder nacional.

4.4 CAPACIDADES DA INTELIGÊNCIA DA AMEAÇA

4.4.1 Os métodos usados pela ameaça correspondem à forma como este ator empregará seus recursos, materiais e humanos, nas diversas frações de Intlg, para levantar as informações críticas em uma operação militar.

4.4.2 Para isso, a ameaça estudará a capacidade das F Ami, suas vulnerabilidades e limitações.

4.4.3 A capacidade de obtenção refere-se ao modo que uma ameaça empregará seus sensores, durante uma situação de guerra, para obter dados sobre o ambiente operacional, poder de combate e Intlg F Ami.

4.4.4 Essas capacidades podem empregar os seguintes meios de Intlg:

- a) Operadores de Inteligência Humana (HUMINT) para obter dados em todo o espaço de batalha;
- b) Sensores de Inteligência Cibernética (CIBERINT) no ambiente cibernético;
- c) Sensores de Inteligência de Sinais (SIGINT) no espectro eletromagnético;
- d) Sensores de Inteligência de Imagem (IMINT) no ambiente de imagens;
- e) obtenção de dados que não são protegidos e podem ser encontrados em Serviço de Inteligência sobre Fontes Abertas (OSINT);
- f) Inteligência de Saúde (MEDINT) para obter dados relativos à saúde humana ou animal;
- g) extração de dados por meio de materiais e equipamentos usados pela tropa amiga por meio da Inteligência Técnica (TECHINT);
- h) obter informações operacionais sobre alvos compensadores por meio da Inteligência por Assinatura de Alvos (MASINT); e
- i) tropa, comum ou especial, como sensor de dados e informações em operações.

4.4.5 Para negar informações à ameaça, é necessário conhecer quais são as técnicas que ela utiliza no ambiente operacional, visando a atender suas NI. As seguintes possibilidades de obtenção podem ser utilizadas pela ameaça:

- a) observação direta – qualquer tropa inimiga em contato, com boa consciência situacional, pode ser um sensor de Intlg e levantar informações acerca das NI determinadas pelo escalão superior;
- b) elementos especializados – unidades especializadas em realizar missões de reconhecimento, tais como tropas mecanizadas, de reconhecimento e vigilância e de operações especiais, utilizando para isso seus meios orgânicos;

- c) captura de prisioneiros de guerra e refugiados – utiliza-se como fonte de informação em razão de sua situação de extrema vulnerabilidade, o que facilita o levantamento de dados;
- d) transmissões eletromagnéticas – utilização do espectro eletromagnético para capturar informações sobre as comunicações em combate, bem como para obter a localização de tropas e os sistemas de sensores. Deve-se levar em conta qual país controla as comunicações regulares da área de conflito;
- e) atividades cibernéticas – o meio cibernético pode ser utilizado para levantar diversas informações acerca de limitações, capacidades, localização, movimentação das tropas empregadas, bem como das instalações ocupadas;
- f) imageamento – a ameaça pode ter à disposição ferramentas de produção de imagens, tais como satélites, aeronaves e Sistemas de Aeronaves Remotamente Pilotadas (SARP) que lhe permitam produzir imagens sobre o ambiente operacional e, assim, melhorar a consciência situacional acerca do seu oponente. As informações levantadas podem conter dados sobre equipamentos empregados, dispositivo da tropa, localização, bem como as atividades desenvolvidas no campo de batalha;
- g) documentação e material – os documentos e materiais abandonados, capturados ou perdidos em campo de batalha podem possuir informações acerca do Dispositivo, Composição, Valor, Atividades Importantes, Peculiaridades e Deficiências (DiCoVaP) da tropa;
- h) noticiário e órgãos de mídia – informações acerca do ambiente operacional nos campos político, econômico, psicossocial e militar podem ser difundidas em noticiários por meio de redes de televisão, rádio e redes sociais;
- i) indiscrição – indiscrição de combatentes e não combatentes, no ambiente operacional e em seu entorno, em comunicações particulares (telefones celulares, uso de redes sociais etc.), bem como por meio de conversas com estranhos, podendo assim revelar, ainda que de forma não intencional, informações críticas ou sensíveis;
- j) emprego de agentes de inteligência e colaboradores – a ameaça pode ter a capacidade de infiltrar elementos da fonte humana no ambiente operacional, bem como cooptar colaboradores e informantes na área de operações que cooperem com informações para atender a seus objetivos; e
- k) população em geral – populares podem ser induzidos (por meio de propaganda ou ação psicológica, motivados conforme sua necessidade ou até mesmo forçados) a colaborar com informações sobre os eventos no ambiente operacional.

CAPÍTULO V

ANÁLISE DAS VULNERABILIDADES

5.1 CONSIDERAÇÕES GERAIS

5.1.1 Este capítulo refere-se à 3ª fase do PSIOp, que visa a analisar as vulnerabilidades das F Ami no ambiente operacional diante das capacidades e ações das ameaças.

5.1.2 Entende-se por **vulnerabilidade** a deficiência que, ao ser explorada pela ameaça, pode causar incidentes de segurança e gerar impactos negativos.

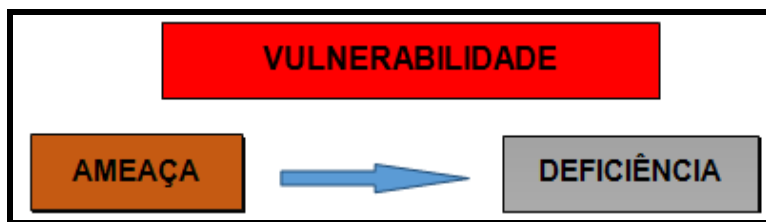


Fig 5-1 – Síntese do conceito de vulnerabilidade

5.1.3 Conforme a Fig 5-1, que sintetiza a concretização de uma vulnerabilidade, esta somente será efetiva pela ação da **ameaça** (ator + motivação + capacidade de agir) em alguma **deficiência** das F Ami (incapacidade de deter/minimizar a ação da ameaça). Dito isso, este capítulo será a base do PSIOp.

5.1.4 Uma vez identificadas as ameaças e o conjunto de deficiências existentes, deverão ser mapeadas e analisadas as vulnerabilidades que influenciarão a Seg Info Op. Essas atividades auxiliarão os planejadores a estabelecer medidas para priorizar seus esforços de segurança e a reduzir seus riscos mais eficazmente.

5.1.5 O domínio e a manipulação das informações em combate, quando empregados pela ameaça, terão as seguintes finalidades:

- a) destruir ou degradar o Comando e Controle (C²);
- b) destruir ou enganar o reconhecimento, a vigilância e a aquisição de alvos;
- c) negar compreensão situacional;
- d) isolar elementos-chave de uma força oponente; e
- e) distorcer ou negar informações a atores e públicos relevantes.

5.1.6 As vulnerabilidades na segurança da informação constituem um ponto crucial para a proteção de dados no ambiente operacional. Elas representam

fraquezas ou falhas que, se exploradas por ameaças, podem resultar no comprometimento da integridade, confidencialidade ou disponibilidade das informações.

5.1.7 A seguir serão apresentadas algumas deficiências nas Seg Info Op conforme os seus subgrupos de medidas: Seg Info Op no Pessoal; Seg Info Op no Material; Seg Info Op na Documentação; Seg Info Op nas Áreas e Instalações; e Seg Info Op nos MTIC.

5.2 VULNERABILIDADES NA SEGURANÇA DA INFORMAÇÃO NO PESSOAL

5.2.1 Esse subgrupo é destinado a assegurar comportamentos e procedimentos, na tropa empregada, adequados à proteção de dados e informações críticas sobre as operações militares.

5.2.2 Entre as deficiências por parte das tropas amigas, destacam-se as seguintes falhas:

- a) acesso a *links* suspeitos que possam obter dados sobre operações militares;
- b) uso indevido de redes sociais para a tramitação de informações operacionais;
- c) sofrer influência de atores externos que possam modificar o comportamento humano;
- d) manipular ou difundir, de forma indevida, documentos operacionais sensíveis ou sigilosos;
- e) compartilhar informações operacionais por indiscrição, erro ou de forma intencional;
- f) inobservância de regras de sigilo e de conduta por parte dos elementos integrantes de áreas sensíveis;
- g) usar equipamentos pessoais que contenham informações críticas para as operações, como celular, relógio, *tablets*, computadores etc.;
- h) ser capturado e prover informações operacionais à ameaça;
- i) perder, extraviar ou entregar material militar a público desconhecido;
- j) permitir ações de HUMINT da ameaça junto a combatentes e não combatentes que tenham acesso às áreas e instalações que detêm informações operacionais relevantes;
- k) inadequado treinamento para uso de equipamentos militares de comunicações e guerra eletrônica;
- l) grupos populacionais e atores relevantes que possam ser alvos da Intlg da ameaça; e
- m) processos frágeis de recrutamento, instrução, credenciamento de segurança e desmobilização.

5.3 VULNERABILIDADES NA SEGURANÇA DA INFORMAÇÃO NO MATERIAL

5.3.1 O material, em razão da sensibilidade das informações nele contidas, pode tornar-se alvo permanente das ações hostis. Com isso, todo material que utilize ou veicule informações que, de posse de atores de qualquer natureza, possam implicar riscos para a missão deve ser protegido.

5.3.2 A ameaça poderá empregar a Inteligência Técnica para realizar a “engenharia reversa” e obter dados que podem ser usados para degradar ou inutilizar sistemas de armas e equipamentos das F Ami.

5.3.3 Exemplos de deficiências que podem ser exploradas pela ameaça:

- a) material criptográfico sem dispositivos de proteção/destruição em equipamentos passíveis de serem perdidos, abandonados ou capturados;
- b) falha nos procedimentos de armazenamento do material;
- c) falha na destruição ou descarte inadequado de materiais sensíveis;
- d) falhas quanto à adoção de medidas de segurança no emprego dos materiais, tais como uso de técnicas de camuflagem, dispersão e guarda do material;
- e) transporte inadequado de materiais de alto valor agregado, tanto na embalagem para transporte como na segurança ostensiva;
- f) perda ou captura de sistema de armas, apoio de fogo ou C², drones, aeronaves, viaturas etc.; e
- g) uso de equipamentos não autorizados.

5.4 VULNERABILIDADES NA SEGURANÇA DA INFORMAÇÃO NA DOCUMENTAÇÃO

5.4.1 Os documentos constituem o suporte mais comum das informações. Nesse sentido, tornam-se alvos permanentes das ações hostis, de modo que podem ser explorados pela Intlg da ameaça.

5.4.2 No tocante à Seg Info na documentação, são exemplos de deficiências que podem ser exploradas pelas ameaças:

- a) armazenamento de documentos sensíveis em equipamentos portáteis;
- b) a falta de controle dos recursos utilizados na produção de documentos sensíveis;
- c) manejo inadequado de cartas e planos de operações militares;
- d) vazamento de planos de voo de aeronaves pilotadas e SARP;
- e) imagens de cartas de situação e operacionais mal protegidas na fase de difusão e transmissão;
- f) falta de cuidado na exposição dos manuais de campanha, seja fisicamente ou virtualmente;

- g) condutas viciadas no trâmite de documentação operacional, como pessoas não credenciadas e trato indevido das informações;
- h) falhas nos procedimentos de controle de segurança na tramitação das documentações atinentes às operações;
- i) locais e processos inadequados de arquivamento, destruição e recuperação dos documentos sigilosos; e
- j) descontinuidade e/ou vazamento de dados durante o ciclo de vida da documentação.

5.5 VULNERABILIDADES DA SEGURANÇA DA INFORMAÇÃO NAS ÁREAS E INSTALAÇÕES

5.5.1 As áreas e instalações críticas de combate e de apoio ao combate podem conter informações possíveis de serem exploradas pelas ameaças, por meio de ações hostis, com uso de meios cibernéticos, ópticos, eletrônicos, operadores de Intlg, dentre outros.

5.5.2 Como exemplo de deficiências na proteção de informações de áreas e instalações a serem protegidas, cabe destacar:

- a) medidas de proteção insuficientes de áreas ou instalações que possibilitem o sensoriamento de imagens desses locais pela ameaça;
- b) falhas no controle das informações em áreas ou instalações que indiquem a localização de arquivos digitais ou documentos físicos;
- c) deficiências nas instalações de C² e de logística que indiquem sua localização;
- d) medidas do plano de defesa de instalações sensíveis que indiquem informações sobre sua execução;
- e) falhas nas medidas de contraespionagem, camuflagem, simulação e dissimulação de áreas e instalações que exponham informações sobre esses locais; e
- f) falhas no controle dos locais de entrada de pessoas e de veículos às instalações sensíveis, como postos de comando, bases militares e estruturas logísticas, possibilitando o acesso às suas informações.

5.6 VULNERABILIDADES NA SEGURANÇA DA INFORMAÇÃO NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES (MTIC)

5.6.1 As informações nos MTIC são ativos valiosos de uma organização, pois grande parte delas está armazenada e são transmitidas por meios eletrônicos em um ambiente volátil, incerto, complexo e ambíguo.

5.6.2 Como exemplos de deficiência na segurança das informações, nos MTIC, mais suscetíveis de serem exploradas pelas ameaças, destacam-se:

- a) falha no uso de criptografia, seja por voz ou dados e mensagens preestabelecidas;
- b) difusão de informações sensíveis das operações por aplicativos de mensagens instantâneas;
- c) utilização de aparelhos celulares como repositórios de dados e informações sensíveis;
- d) fragilidade na adoção de normas de segurança compatíveis para armazenamento e trâmite de dados por meios eletrônicos;
- e) falta de manutenção regular e atualizações de *softwares*;
- f) utilização de redes *wifi* em operações sem segurança;
- g) emprego de dispositivos eletrônicos pessoais em operação;
- h) falha na segmentação da rede e controle dos níveis de acesso;
- i) ausência de armazenagem externa de dados (*backup*) de maneira efetiva e sistemática;
- j) possibilidade de ações de sabotagem/ataque nas estruturas de C², comprometendo significativamente a capacidade de coordenação das operações;
- k) emissão de sinais eletromagnéticos oriundos de sistema de radares e equipamentos satelitais, possibilitando sua geolocalização;
- l) sensores de vigilância e aquisição de alvos rastreáveis e/ou sem proteção sob vistas aéreas;
- m) centros de C² passíveis de interrupções e contramedidas de Com;
- n) falha no processo das comunicações, pelo gerenciamento inadequado da informação que poderá causar falta de entendimento da situação, confusão, desperdício de tempo, sobrecarga de trabalho ou até retrabalho;
- o) falta de objetividade, simplicidade e oportunidade na tramitação de informações no TO;
- p) fragilidade ou insuficiência dos sistemas e infraestrutura de telecomunicações;
- q) falta ou falha de campanhas de conscientização, junto à tropa empregada e aos seus familiares/amigos, acerca dos ativos a serem preservados e protegidos, devendo estar restritos apenas às redes de comunicação seguras, não sendo plausível o trâmite de informações sensíveis em mídias sociais;
- r) falha na comunicação segura e restrita entre combatentes e seus familiares/amigos durante as operações militares; e
- s) vazamento ou interceptação de sinais de receptores de radiofrequência, dispositivos de comunicação e protocolos de informação.

5.6.3 EMPREGO DAS MÍDIAS SOCIAIS

5.6.3.1 O emprego da internet e, particularmente, das redes sociais tem aumentado consideravelmente a coleta de dados operacionais pelas ameaças, que são publicados por combatentes e por não combatentes. O perigo dessa exposição é justamente o tipo de dado que está sendo exposto, pois, ao

veicular dados relacionados às operações em curso ou futuras, pode-se comprometer a segurança das informações de forma parcial ou total.

5.6.3.2 As mídias sociais são usadas, intencional, errônea e, por vezes, não intencionalmente, para informar a disposição e a composição de forças militares, o estado da infraestrutura e os detalhes de acontecimentos locais em curso, representando um grande risco para as atividades militares das F Ami. Esses dados poderão comprometer decisivamente as operações militares.

5.6.3.3 O uso da Inteligência de Fontes Abertas (OSINT) para monitorar redes sociais se configura em uma prática adotada por ambos os lados do conflito. Mas a mitigação dos riscos associados às mídias sociais é complexa e apresenta desafios significativos em termos de regulação e controle.

5.6.3.4 A natureza dinâmica e amplamente acessível das redes sociais torna difícil prevenir a disseminação de informações sensíveis ou enganosas, exigindo abordagens inovadoras e contínuas para gerenciar e minimizar os impactos dessas plataformas no contexto do conflito.

5.6.3.5 Como exemplo de técnicas e dados empregados para obtenção de informações em mídias sociais, podem ser citados:

- a) *geotagging* – é o processo de obter coordenadas geográficas contidas em mídia social, permitindo a localização de um dispositivo móvel. As *geotags* podem ser obtidas de fotos, vídeos, *sites*, mensagens de texto e códigos QR e também podem incluir carimbos de data/hora ou outras informações contextuais;
- b) georreferenciamento – é o processo para definir a forma, a dimensão e a localização, atribuindo coordenadas geográficas a objetos ou dados, vinculando essas informações a um sistema de coordenadas;
- c) *web scraping* (raspagem de dados) – é uma forma de mineração que permite a extração de dados de sites da *web*, convertendo-os em informação estruturada para posterior análise;
- d) análise de sentimentos – é um tipo de análise de dados que está sendo cada vez mais utilizada pelas organizações, com intuito de analisar textos (como *e-mails*, *chats* de atendimento, comentários, etc.), para obter informações sobre sua audiência e entender melhor os anseios do seu público; e
- e) análise léxica – é a primeira etapa do processo de compilação, e seu objetivo é dividir o código fonte em símbolos léxicos, preparando-o para a análise dos dados.

5.6.3.6 Os combatentes e não combatentes munidos de *smartphones*, dispositivos internos de GPS e contas em mídias sociais divulgam, sem saber, informações úteis para a tomada de consciência situacional do combate, como, por exemplo, efetivos militares empregados, infraestruturas bélicas e de apoio, acontecimentos em curso e opinião geral da população.

5.6.3.7 Os dispositivos eletrônicos pessoais representam um risco significativo de segurança operacional para as F Ami.

5.6.3.8 O emprego da análise de sentimentos pode ser exemplificado quando os analistas estudam as postagens nas mídias sociais de quem está dentro do TO, antes e depois das ações de combate, podendo, assim, concluir sobre as opiniões, críticas e “sentimentos” da população local, que redundarão em apoio ou não ao emprego da tropa.

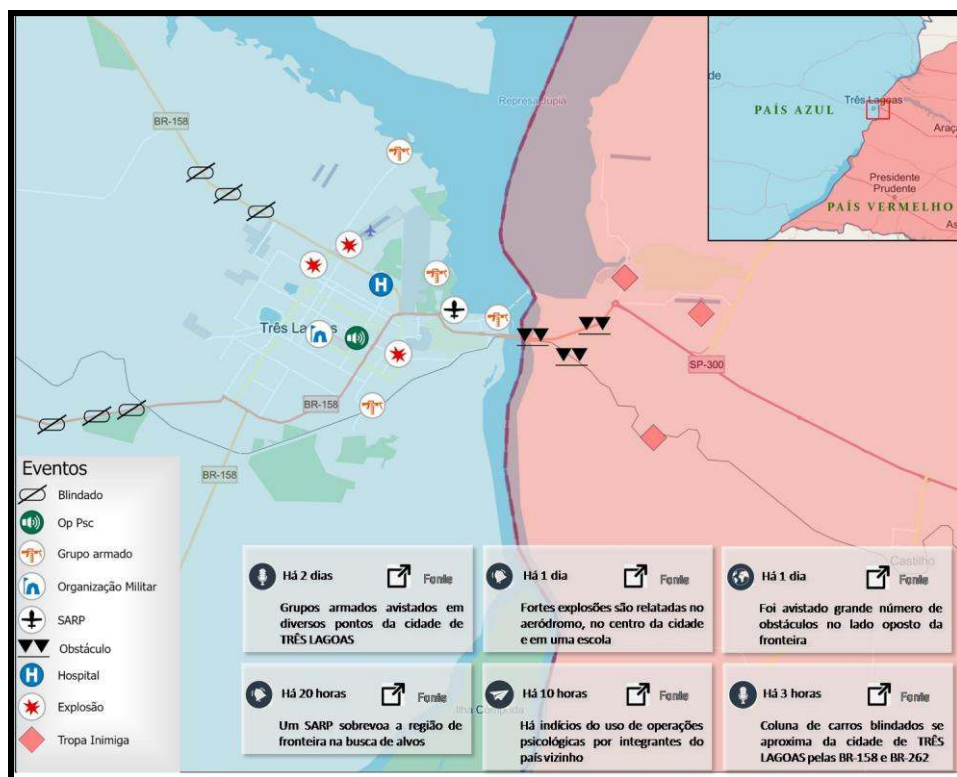


Fig 5-2 – Imagem georreferenciada de exercício militar (exemplo não real)

5.6.3.9 Os analistas podem usar uma combinação de diversos aplicativos, como *Google Maps*, *Wikimapia*, *Instagram*, *tuites* disponíveis publicamente, postagens em mídias sociais, como *Facebook* e *YouTube*, para identificar os locais exatos de ações militares em curso.

CAPÍTULO VI

AVALIAÇÃO DOS RISCOS NA SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

6.1 VISÃO GERAL

6.1.1 Este capítulo refere-se à 4ª fase do PSIOp, que tem como objetivo avaliar os riscos para a Seg Info Op.

6.1.2 Uma vez determinadas e priorizadas as IC que devem ser protegidas, suas ameaças e vulnerabilidades, a fase de “Avaliação de Riscos” determina quais riscos podem afetar a segurança da informação.

6.1.3 A avaliação do risco é mensurada por intermédio da estimativa da capacidade do inimigo em explorar uma vulnerabilidade e dos impactos ou efeitos potenciais que tal exploração terá nas operações.

6.1.4 Se a vulnerabilidade será explorada com sucesso, vai depender da capacidade da Inteligência, da intenção da ameaça e da oportunidade de explorar a vulnerabilidade. Ao considerar todas as vulnerabilidades identificadas, será estimada a probabilidade de ocorrência.

6.1.5 A probabilidade de exploração bem-sucedida e o potencial impacto adverso podem, então, ser considerados para estimar o nível de risco.

6.1.6 Os riscos são analisados de maneira qualitativa. Para isso, são utilizados critérios preestabelecidos com uma escala para determinar o nível de cada risco. A metodologia a ser utilizada possui dois parâmetros claros a serem considerados: probabilidade e impacto.

6.2 AVALIAÇÃO DE PROBABILIDADE

6.2.1 A tabela 6-1 – “Avaliação de Probabilidade” apresenta exemplos de descrições e indicadores a serem considerados para o estabelecimento da probabilidade de ocorrência de cada risco. Para tanto, são priorizados os indicadores julgados preponderantes, de acordo com as especificidades da IC.

PROBABILIDADE DE ATUAÇÃO DA AMEAÇA	
NÍVEL	DESCRIÇÃO E CRITÉRIOS
IMPROVÁVEL	a. <u>Descrição</u> - Evento extraordinário para os padrões conhecidos. - Não há histórico recente sobre a sua ocorrência em operações militares. b. <u>Indicadores</u> - Probabilidade de ocorrência: < 20%. - Motivação do ator: não identificada. - Fragilidade/deficiência: não identificada. - Poder de combate: mínimo. - Nível emprego da Intlg: desconhecido ou básico. - Comando e Controle (C²): desconhecido ou básico. - Sensores (tropa, radar, satélite, GE, CIBER): não possui ou não empregou. - Técnicas, Táticas e Procedimentos (TTP): não identificadas. - A Op extremamente favorável para o emprego da tropa ou extremamente desfavorável às ameaças.
RARAMENTE	a. <u>Descrição</u> - Evento casual, inesperado. Muito embora seja raro, há histórico de sua ocorrência em operações. b. <u>Indicadores</u> - Probabilidade de ocorrência: > 20% RARO < 40%. - Motivação do ator: baixa. - Fragilidade/deficiência: pouca, inexpressiva, pouco vantajosa. - Poder de Combate: baixo. - Nível emprego da Intlg: básico. - Comando e Controle (C²): básico. - Sensores (tropa, radar, satélite, GE, CIBER): possui e não se sabe detalhes. - Técnicas, Táticas e Procedimentos (TTP): elementar. - A Op favorável para o emprego da tropa ou desfavorável às ameaças.
OCASIONAL	a. <u>Descrição</u> - Evento esperado. Ocorre com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento do Cmdo enquadrante em operações. b. <u>Indicadores</u> - Probabilidade de ocorrência: > 40% OCASIONAL < 60%. - Motivação do ator: média. - Fragilidade/deficiência: há médias deficiências que podem ser exploradas. - Poder de combate: médio ou equivalente. - Nível emprego da Intlg: médio ou equivalente.

PROBABILIDADE DE ATUAÇÃO DA AMEAÇA	
NÍVEL	DESCRIÇÃO E CRITÉRIOS
	- Comando e Controle (C²): mediano. - Sensores (tropa, radar, satélite, GE, CIBER): possui e tem capacidade em empregar. - Técnicas, Táticas e Procedimentos (TTP): adestrada. - A Op favorável equilibrada para o emprego da tropa amiga ou pela ameaça.
PROVÁVEL	a. <u>Descrição</u> - Evento usual, corriqueiro. Seu histórico é amplamente conhecido pelo Cmdo enquadrante em operações. b. <u>Indicadores</u> - Probabilidade de ocorrência: > 60% PROVÁVEL < 80%. - Motivação do ator: alta. - Fragilidade/deficiência: deficiências e vulnerabilidades das F Ami levantadas e que serão exploradas. - Poder de combate: equivalente ou maior. - Nível emprego da Intlg: equivalente ou maior. - Comando e Controle (C²): equivalente ou maior. - Sensores (tropa, radar, satélite, GE, CIBER): possui e emprega com capacidade equivalente ou maior. - Técnicas, Táticas e Procedimentos (TTP): adestramento avançado. - A Op desfavorável para o emprego da tropa amiga ou favorável à ameaça.
FREQUENTE	a. <u>Descrição</u> - Evento se reproduz muitas vezes, frequentemente. - Interfere contundentemente no curso das operações das F Ami. b. <u>Indicadores</u> - Probabilidade de ocorrência: FREQUENTE > 80%. - Motivação do ator: muito alta. - Fragilidade/deficiência: deficiências e vulnerabilidades extremas das F Ami exploradas com frequência. - Poder de combate: maior. - Nível emprego da Intlg: maior. - Comando e Controle (C²): maior. - Sensores (tropa, radar, satélite, GE, CIBER): emprega com elevada capacidade. - Técnicas, Táticas e Procedimentos (TTP): muito adestrada. - A Op extremamente desfavorável para o emprego da tropa amiga ou muito favorável à ameaça.

Tab 6-1 – Avaliação da Probabilidade

6.3 AVALIAÇÃO DE IMPACTO

6.3.1 A tabela 6-2 apresenta exemplos de descrições e indicadores a serem considerados para o estabelecimento do impacto de cada risco, avaliando superioridade, inferioridade e igualdade das forças.

6.3.2 Para tanto, são priorizados os indicadores julgados preponderantes, de acordo com as especificidades da IC, a qual pode criar outros indicadores, conforme a situação específica.

IMPACTO	
NÍVEL	DESCRIÇÃO E INDICADORES
BAIXO	a. <u>Descrição</u> - Impactos pequenos nos ativos de informações operacionais das F Ami. - Não compromete a Seg Info Op. b. <u>Indicadores</u> (sem degradação para cumprir a missão) - Cumprimento da missão: sem reflexos negativos. - Poder de combate: sem redução. - Nível de prontidão: sem redução. - Comando e controle: sem avaria/interrupção. - Perdas humanas e materiais: baixas perdas humanas e em MEM. - Danos nos sensores de obtenção: sem danos. - Danos colaterais: pequena proporção, não identificados não combatentes feridos ou instalações civis destruídas (hospitais, escolas etc.).
MODERADO	a. <u>Descrição</u> - Impactos significativos nos ativos de informações operacionais das F Ami, porém recuperáveis. - Interfere na Seg Info Op, requer medidas de proteção e prevenção. b. <u>Indicadores</u> (degradação de até 20%) - Cumprimento da missão: reflexos diretos, embora seja manobrável sem interferir na missão. - Poder de combate: redução média, recuperável em pouco tempo. - Nível de prontidão: redução média, recuperável em pouco tempo. - Comando e controle: avaria/interrupção, recuperável em pouco tempo. - Perdas humanas e materiais: significativas perdas humanas e em MEM, com possível reacompanhamento em curto prazo.

IMPACTO	
NÍVEL	DESCRIÇÃO E INDICADORES
	- Danos nos sensores de obtenção: danos parciais, recuperáveis. - Danos colaterais: danos visíveis em não combatentes (feridos ou mortos) e instalações civis destruídas (hospitais, escolas etc.).
CRÍTICO	a. <u>Descrição</u> - Impactos de reversão muito difícil nos ativos de informações operacionais das F Ami. - Interfere decisivamente na Seg Info Op, requer medidas urgentes de recuperação e contenção da ameaça. b. <u>Indicadores</u> (degradação de até 30%) - Cumprimento da missão: reflexos graves e pode comprometer decisivamente a missão. - Poder de combate: redução significativa, recuperável em tempo médio. - Nível de prontidão: redução alta, recuperável em tempo médio. - Comando e controle: avaria/interrupção, de difícil recuperação e em tempo médio. - Perdas humanas e materiais: alto grau de perdas humanas e em MEM, com difícil reacompletamento e em prazo médio. - Danos nos sensores de obtenção: danos críticos, há perdas irreparáveis, necessitando reparo ou troca de grande parte dos sensores. - Danos colaterais: número significativo de não combatentes feridos ou mortos e inúmeras instalações civis destruídas (hospitais, escolas etc.).
CATASTRÓFICO	a. <u>Descrição</u> - Há impactos permanentes nos ativos de informações operacionais das F Ami. - Ameaça detém o controle da maioria das IC das F Ami, requer obtenção de novas capacidades para reverter o quadro. b. <u>Indicadores</u> (degradação de 30% a 50%) - Cumprimento da missão: reflexos gravíssimos, acarretando o não cumprimento da missão pelas F Ami. - Poder de combate: sem poder de combate para restabelecer o contato, não recuperável. - Nível de prontidão: redução altíssima, recuperável em longo tempo. - Comando e controle: avaria/interrupção de difícil recuperação em longo tempo.

IMPACTO	
NÍVEL	DESCRIÇÃO E INDICADORES
	- Perdas humanas e materiais: gravíssimas perdas humanas e em MEM, de muito difícil re completamento e em longo prazo. - Danos nos sensores de obtenção: vários danos irreversíveis, algumas perdas irreparáveis, necessitando troca de grande parte dos sensores. - Danos colaterais: perdas indiscriminadas e em grande número de não combatentes e ataques indiscriminados de instalações civis (hospitais, escolas etc.).

Tab 6-2 – Avaliação de Impacto

6.4 NÍVEL DO RISCO

6.4.1 O nível do risco é estabelecido mediante o emprego da Matriz de Avaliação de Risco. Para tanto, cruza-se a probabilidade com o impacto.

6.4.2 A Matriz demonstra a relação entre probabilidade e impacto. Essas duas dimensões de risco, quando combinadas, resultam em um terceiro elemento de risco denominado Nível de Risco (baixo, médio, alto e extremo).

MATRIZ DE AVALIAÇÃO DE RISCO		PROBABILIDADE (FREQUÊNCIA)				
		FREQUENTE	PROVÁVEL	OCASIONAL	RARAMENTE	IMPROVÁVEL
		> 80%	60% a 80%	40% a 60%	20% a 40%	<20%
IMPACTO (GRAVIDADE)		V	IV	III	II	I
CATASTRÓFICO: falha da missão; prontidão da unidade eliminada; perda de poder de combate; significativas perdas humanas ou materiais; dano inaceitável.	IV	E	E	A	A	M
CRÍTICO: prontidão da OM degradada; comprometimento da capacidade de combater; lesões severas; doenças; grandes perdas humanas ou materiais; dano inaceitável.	III	E	A	A	M	B
MODERADO: prontidão da OM com degradação média; capacidade de combater pouco comprometida; poucos ferimentos; doenças; poucas perdas humanas ou materiais; danos controláveis.	II	A	M	M	B	B
BAIXO: impacto baixo para a prontidão ou capacidade de combater; mínimas ocorrências de ferimentos, doenças, perdas ou danos.	I	M	B	B	B	B
NÍVEIS DE RISCO		INDICADORES				
EXTREMO	ALTO	MÉDIO	BAIXO	Impacto (para as F Ami)		Probabilidade (da ameaça atuar)
				-Cumprimento da missão -Poder de combate -Nível de prontidão -Comando e controle -Perdas humanas e materiais -Danos nos Sensores de obtenção -Danos colaterais		-Poder de combate -Nível emprego da Inteligência -Comando e controle (C²) -Sensores (tropa, radar, satélite, GE, CIBER) -Técnicas , Táticas e Procedimentos (TTP).

Fig 6-1 – Matriz de Avaliação de Risco

6.4.3 Os indicadores de impacto para as F Ami e de probabilidade da ameaça atuar, descritos na Fig 6-1, devem estar relacionados obrigatoriamente com a segurança das informações em operações militares.

6.4.4 Os níveis de risco são estabelecidos mediante a combinação das dimensões probabilidade x impacto, conforme a seguir.

a) Área Vermelha – riscos extremos, que exigem a implementação imediata das ações de proteção e prevenção. São eventos que devem ser monitorados prioritariamente.

b) Área Laranja – riscos altos, que devem gerar respostas rápidas, planejadas e testadas em planos de segurança. São eventos que devem ser constantemente monitorados.

c) Área Amarela – riscos médios, que devem ser monitorados de forma rotineira e sistemática, reforçando as ações de prevenção e proteção.

d) Área Verde – riscos baixos, que representam pequenos danos. Esses riscos podem ser somente gerenciados e administrados.

6.4.5 Possíveis mudanças na probabilidade ou no impacto afetam os níveis de risco, ou seja, pode haver migração do risco.

6.4.6 Ressalta-se que, nessa fase do Processo de Seg Info Op, a prioridade máxima de avaliação será as informações críticas.

6.5 CLASSIFICAÇÃO DO RISCO

6.5.1 A tabela 6-3 apresenta a classificação dos níveis de riscos e as providências decorrentes, a fim de orientar seu tratamento futuro.

CLASSIFICAÇÃO (NÍVEL)	ÁREA	PROVIDÊNCIAS
EXTREMO	VERMELHA	Ação imediata
ALTO	LARANJA	Ação no curto prazo
MÉDIO	AMARELA	Ação no médio prazo
BAIXO	VERDE	Risco controlável

Tab 6-3 – Classificação do risco e providências

6.5.2 Os riscos são numerados (código do risco), a fim de facilitar o seu monitoramento e controle, inclusive quanto às possíveis mudanças de sua ordem de prioridade. Os riscos são levantados com o auxílio da tabela apresentada (exemplo) a seguir.

SEGURANÇA DAS INFORMAÇÕES							
SUBGRUPO DE MEDIDAS ÁREAS E INSTALAÇÕES							
IDENTIFICAÇÃO DA INFORMAÇÃO CRÍTICA (IC) LOC DA Z REU DA TROPA BLINDADA							
CÓD RISCO (2)	VULNERABILIDADES POSSÍVEL LOCALIZAÇÃO DE TROPA POR MEIO DE SARP OU FONTES HUMANAS						
	AMEAÇA			DEFICIÊNCIAS (6)	ANÁLISE		AVALIAÇÃO
	Ator (3)	Ação (4)	Motivações (5)		Probabilidade (7)	Impacto(8)	
IC 1	Intlg Imagem (IMINT)	Sobrevôo SARP	Deter/destruir Tropa Bld	Não ter capacidade de camuflar/ocultar local de reunião de tropa	PROVÁVEL	CRÍTICO	ALTO
IC 2	Intlg F Hum (HUMINT)	Infiltração na Z Reu	Identificar Loc e Poder de Cmb	Falta de medidas de Seg física e tecnológica	RARAMENTE	MODERADO	BAIXO

Tab 6-4 – Definição dos Riscos

- (1) Elaborar as tabelas de avaliação de riscos, separando-as por subgrupos de medidas da Segurança da Informação.
- (2) Numerar cada risco.
- (3) Relacionar os atores com capacidade para realizar ações hostis sobre os ativos a serem protegidos, destacando os impactos visualizados.
- (4) Para cada ator, relacionar as ações que podem afetar os ativos a serem protegidos (uma ação por linha).
- (5) Relacionar as motivações do ator para realizar cada ação hostil.
- (6) Relacionar às deficiências levantadas, podendo agrupá-las, de acordo com a ameaça considerada.
- (7) Qualificar a probabilidade de ocorrência da ação, conforme a Avaliação de Probabilidade (Tab 6-2).
- (8) Qualificar o impacto, conforme a Avaliação de Impacto (Tab 6-3).
- (9) Qualificar o risco, conforme a Matriz de Avaliação de Riscos (Fig 6-1).

6.5.3 Para a definição dos riscos, deverão ser priorizados os indicadores constantes da Fig 6-1, pois provavelmente estarão relacionados com as informações críticas a proteger.

CAPÍTULO VII

PLANEJAMENTO DA SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

7.1 CONSIDERAÇÕES GERAIS

7.1.1 Este capítulo tem por objetivo finalizar o Processo de Seg Info Op na orientação da execução de sua 5ª fase – “Aplicar Medidas de Segurança das Informações nas Operações”.

7.1.2 O Plano da Seg Info no âmbito das operações militares é o produto final e fará uso de todos os produtos das fases anteriores. Cabe ressaltar que o PSIOp deve ser atualizado durante o conflito armado, em cada fase das operações.

7.1.3 Cabe destacar que o desenvolvimento da mentalidade de segurança das informações em operações é essencial para que o plano de Seg Info Op possa ser efetivo. Para tal, é necessário que alguns fundamentos devam ser atendidos, tais como:

- a) cada combatente ou não combatente está exposto de forma física e virtual (atividades funcionais e sociais, reuniões, rotina de trabalho, postagens em mídias sociais, atividades físicas, movimentos de tropa, comunicações etc.);
- b) a ameaça está buscando informações das F Ami permanentemente (contato direto, indireto, não hostil, químico, biológico, radiológico e nuclear, aéreo, visual e eletromagnético);
- c) entenda e acompanhe as ameaças às F Ami (capacidade de identificar fisicamente ou virtualmente as ameaças, protegendo as operações e os combatentes de forma contínua); e
- d) empregue medidas de segurança ativa e passiva de Seg Info (operações de contra reconhecimento e defesa do ciberespaço, camuflagem, ruído e disciplina de luz; fortalecimento da infraestrutura crítica; e redução das emissões eletromagnéticas).

7.1.4 A Seg Info Op preconiza etapas de gerenciamento de risco para examinar e auxiliar as fases de planejamento, preparação, execução e pós-execução de qualquer atividade em todo o espectro de ações militares e ambientes operacionais. Esse gerenciamento tem a finalidade de fornecer aos decisores um meio de avaliação dos riscos inerentes às informações críticas que necessitarão intervir em operações.

7.1.5 As Organizações Militares de Inteligência Militar (OMIM) são estruturas que empregam frações específicas para a obtenção de dados em operações militares desde a paz até a guerra.

7.1.6 Nesse sentido, as OMIM estão aptas a executar todas as atividades do processo IRVA, apoiando a obtenção e a manutenção da consciência situacional, proporcionando a desejável superioridade de informações, além de possuir capacidade de realizar a busca por ameaças.

7.1.7 Dentro da estrutura organizacional da F Ter, existem três níveis de OMIM: o Grupamento de Inteligência Militar (Gpt Intlg Mil), que atua em proveito do Corpo de Exército (C Ex); o Batalhão de Inteligência Militar (BIM), que atua em proveito de uma Divisão de Exército (DE); e a Companhia de Inteligência Militar (CIM), que atua no apoio às Brigadas (Bda).

7.1.8 Em operações militares, a Cel Intlg faz parte do EM do escalão considerado, sendo responsável pela realização do Exame de Situação de Inteligência (Exm Sit Intlg¹). A Cel Intlg tem a responsabilidade de formular as L Aç do inimigo, fazendo constar no Anexo de Inteligência ao Plano Operacional.

7.1.9 Simultaneamente, a Cel Intlg realiza o Exame de Situação de Contrainteligência (Exm Sit CI²), que determina e prioriza as possibilidades da Intlg da ameaça e suas repercussões sobre as L Aç das F Ami.

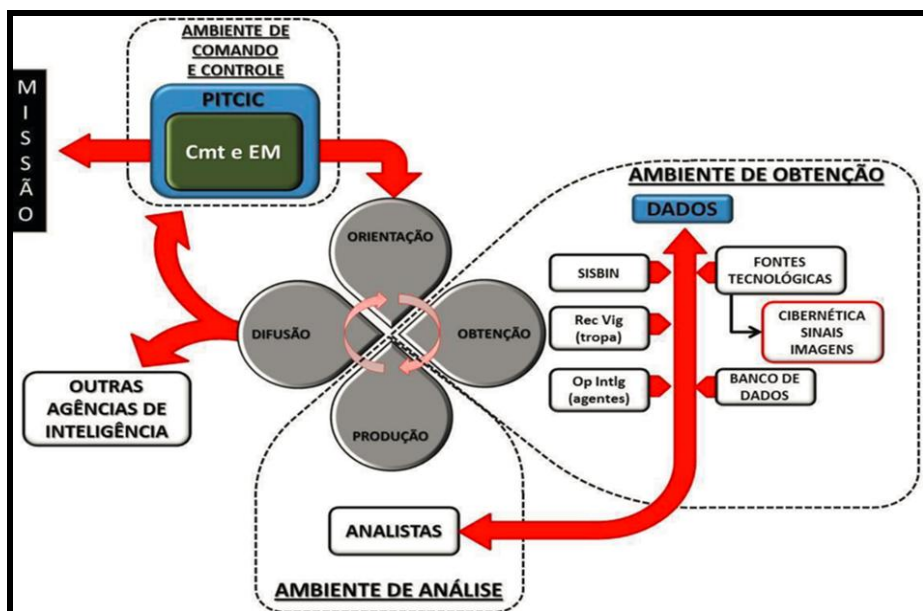


Fig 7-1 – Ambientes de emprego da Intlg

¹Modelo de Exm Sit Intlg – Anexo D ao MC *O Emprego da Inteligência*.

²Modelo de Exm Sit CI – Anexo A – “Memento do Exame de Situação de Contrainteligência” ao MC *Contrainteligência*.

7.1.10 Para o planejamento da Seg Info Op, é necessário considerar as características do ambiente operacional sobre a preparação das operações, o gerenciamento de risco e o processo de desmobilização.

7.1.11 Para execução do Plano de Seg Info Op, serão empregados as estruturas e os militares com encargos relacionados à Intlg de seus escalões. As diretrizes de Seg Info serão difundidas pela cadeia de comando, desde o C Ex até o menor escalão, para difusão junto às tropas em operações e cumprimento das ordens.

7.1.12 Na fase inicial do PSIOp, deverá ser emitida uma Diretriz de Segurança das Informações pela FTC ou pelo maior escalão em presença no TO, contendo:

- a) atribuição de responsabilidades para a Seg Info;
- b) conscientização, educação e treinamento em Seg Info;
- c) processamento correto nas aplicações;
- d) gestão de vulnerabilidades técnicas;
- e) gestão de continuidade, análise contínua;
- f) gestão de incidentes de segurança da informação e melhorias;
- g) mapeamento e acompanhamento das informações críticas.

7.2 O PLANEJAMENTO DA SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

7.2.1 O planejamento das atividades de segurança das informações deve ser um processo contínuo e integrado à execução de todas as operações e atividades.

7.2.2 Está diretamente associado à conscientização quanto as prováveis ameaças, bem como ao treinamento e à qualidade das ações implementadas.

7.2.3 O produto do planejamento será o Plano de Segurança das Informações nas Operações, adendo ao Plano de Contraineligência do escalão respectivo. Esse plano decorre do Exm Sit da Seg Info Op que se baseia no Exm Sit CI.

7.2.4 As atividades desenvolvidas no planejamento da Seg Info Op estão diretamente relacionadas e decorrem dos Exm Sit CI e dos planejamentos de contraineligência realizados nos escalões que conduzem as operações.

7.2.5 Toda informação referente às operações deve ser compartilhada apenas com quem tenha a necessidade de conhecer.

7.2.6 O planejamento para a Seg Info Op é um processo pelo qual os comandantes visualizam as ações necessárias para a preparação e a execução das atividades e tarefas essenciais para salvaguardar os ativos

informacionais. A prática do planejamento maximiza as oportunidades e orienta as dinâmicas de controle em cada fase da operação.

7.2.7 Durante o planejamento, deve ser considerada a LIC, levantada na preparação, para definição das medidas a serem adotadas na redução ou eliminação dos riscos e ameaças às IC.

7.2.8 As ações previstas devem determinar as principais tarefas que as estruturas da cadeia de comando precisam atentar para proporcionar a Seg Info.

7.2.9 Ressalta-se a necessidade de abordar, ainda, as medidas de Seg Info Op durante todas as etapas da desmobilização, pós-conflito.

7.3 DESMOBILIZAÇÃO DAS OPERAÇÕES MILITARES

7.3.1 A desmobilização consiste no conjunto de atividades planejadas para serem executadas após o término da operação. São medidas que visam à Seg Info na pós-missão, evitando que sejam utilizadas de maneira errada e em momento inoportuno.

7.3.2 A desmobilização é composta por ações específicas para a proteção de todos os ativos que contêm informações críticas. O processo está descrito conforme o Plano de Seg Info Op – Apêndice nº 1 ao Anexo B, deste manual.

ANEXO A

MODELO DE EXAME DE SITUAÇÃO DE SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

(GRAU DE SIGILO)

(Rfr: Crt... Esc... Fl...)

Exemplar Nr

Unidade

Local

Data-Hora

Indicativo

EXAME DE SITUAÇÃO DE SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

(Adendo ao Exame de Situação de Contraineligência da FTC)

Referências: listar documentos e cartas utilizados no planejamento.

1. MISSÃO

- Enunciado da missão imposta.

2. CARACTERÍSTICAS DO AMBIENTE OPERACIONAL

- a) Principais Informações Críticas presentes no ambiente operacional.
- b) Informações Críticas das Forças Amigas referentes à Segurança Ativa.
- c) Informações Críticas das Forças Amigas referentes à Segurança da Informação.
 - 1) Segurança do Pessoal
 - 2) Segurança da Documentação
 - 3) Segurança do Material
 - 4) Segurança dos Meios de Tecnologia da Informação
 - 5) Segurança das Áreas e Instalações
- d) Aspectos do terreno
 - Condições climáticas, meteorológicas, características (políticas, econômicas, psicossociais, guerra eletrônica e sensoriamento remoto) e outros aspectos que podem ser explorados pelas ameaças para causar vulnerabilidade na segurança da informação.

- Informações Críticas para a Seg Info Op constantes dos aspectos fisiográficos e dos fatores operacionais.

e) Considerações Civas (AECOPE³ – Informações Críticas)

- Devem ser levantadas as considerações civis que poderão afetar a segurança das informações.

3. SITUAÇÃO DAS AMEAÇAS (organização e estrutura)

- a. Inteligência (estrutura, capacidades e desdobramento no terreno).
- b. Tropa como sensor (operações especiais, operações psicológicas e tropa comum).
- c. Sensores de obtenção de dados.
- d. Expressões do poder nacional da ameaça.
- e. Forças armadas de países aliados.
- f. Forças de coalizão inimiga (eminentemente conjuntas).
- g. Forças não convencionais hostis (grupos insurgentes, organizações terroristas, facções criminosas etc.).
- h. Instituições e agências civis (estatais e não estatais/locais e internacionais).
- i. Companhias militares privadas.
- j. Organizações criminosas.
- k. População local.
- l. Mídias em geral.

4. CAPACIDADES DAS AMEAÇAS

- a. Inteligência
 - Organização, estrutura, capacidades e desdobramento no terreno.
 - Inteligência Humana (HUMINT).
 - Inteligência de Sinais (SIGINT).

³AECOPE – áreas, estruturas, capacidades, organização, população e evento.

- Inteligência Cibernética (CIBERINT).
- Inteligência de Imagens (IMINT).
- Inteligência de Fontes Abertas (OSINT).
- Inteligência de Saúde (MEDINT).
- Inteligência Técnica (TECHINT).
- Inteligência por Assinatura de Alvos (MASINT).

b. Sensores e sistemas de obtenção de dados (guerra eletrônica, radares, drones etc.).

c. Tropa como sensor (operações especiais, operações psicológicas, tropa comum etc.).

d. Ferramentas de Inteligência Artificial e análise de dados.

e. Redes de comunicações seguras.

f. Sistemas de Informação Geoespacial (GIS).

g. Centros de Comando e Controle.

h. Criptografia e Segurança da Informação.

i. Integração de Fontes de Informação.

5. GERENCIAMENTO DO RISCO

- Apresentar a Matriz de Definição dos Riscos (Tab 6-4).

6. MEDIDAS ADOTADAS PARA A DESMOBILIZAÇÃO

- Apresentar as medidas adotadas para a desmobilização das operações militares.

7. CONCLUSÕES

- Apresentar as deficiências da Segurança da Informação nas Operações e as possibilidades de obtenção de informações críticas pelas ameaças, indicando o nível do risco (probabilidade *versus* impacto).

ANEXO B**MODELO DE PLANO DE SEGURANÇA DAS INFORMAÇÕES NAS
OPERAÇÕES (PSIOp)****(GRAU DE SIGILO)**

(Rfr: Crt...Esc...Fl...)

Exemplar Nr

Unidade

Local

Data-Hora

Indicativo

PLANO DE SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES (PSIOp)

(Adendo ao Exame de Situação de Contrainteligência da FTC)

1. SITUAÇÃO**a. Forças Inimigas (ameaças)**

1) Informações críticas das condições climáticas e meteorológicas que podem ser exploradas pelas ameaças para causar danos às Forças Amigas (F Ami).

2) Informações críticas das condições do terreno que podem ser exploradas pelas ameaças para causar danos às F Ami.

3) Características (políticas, econômicas, psicossociais, guerra eletrônica e sensoriamento remoto) e outros aspectos que podem ser explorados pelas ameaças para causar danos às F Ami, com foco nas Informações críticas.

4) Perfil de autoridades – civis e militares.

5) Caracterização da ameaça.

a) Inteligência – organização, doutrina, formas de atuação e principais ações realizadas. Meios com capacidade de levantar Informações críticas das F Ami.

b) Unidades de Operações Especiais (Op sabotagem) – organização, doutrina, formas de atuação e principais ações realizadas.

c) Unidades de operações psicológicas, desinformação e propaganda adversa – organização, doutrina, formas de atuação e principais ações realizadas.

d) Comunicação Social – organização, doutrina, formas de atuação e principais ações realizadas.

e) Guerra Irregular – organização, doutrina, formas de atuação e principais ações realizadas.

f) Grupos Terroristas – organização, doutrina, formas de atuação e principais ações realizadas.

g) Organizações Criminosas – organização, doutrina, formas de atuação e principais ações realizadas.

h) Grupos Hostis – organização, doutrina, formas de atuação e principais ações realizadas.

b. Forças Amigas

1) Informações Críticas das F Ami referentes à Segurança Ativa.

2) Informações Críticas das F Ami referentes à Segurança da Informação (no Pessoal, na Documentação, no Material, nos Meios de Tecnologia da Informação e nas Áreas e Instalações), da Segurança Orgânica.

c. Expressões do Poder Nacional (síntese das capacidades em caso de conflito armado)

- Nesse tópico, devem ser apresentadas as sínteses das narrativas/prioridades de cada expressão do poder nacional em caso de conflito armado, com ênfase nas expressões política e militar.

- Expressões do poder nacional: militar; política; econômica; psicossocial; científica e tecnológica.

Expressão do poder nacional	Fatores a serem priorizados
Militar Explora as capacidades militares e paramilitares de todos os atores relevantes (forças oponente, amiga e neutra).	Doutrina Militar Estrutura militar (organização e articulação) Capacidade de comando e controle Integração das Forças Armadas Instrução, adestramento e aprestamento Moral Militar Capacidade logística Capacidade de mobilização militar Serviço militar Capacidade científica e tecnológica
Política Descreve a distribuição de responsabilidade e poder nos níveis de governo.	Situação geopolítica Condicionantes históricos Doutrinas e ideologias políticas Elites e lideranças políticas
Econômica Analisa o comportamento individual e coletivo quanto à obtenção, distribuição e ao consumo de recursos financeiros.	Modernização e adaptação às mudanças Capacidade de formação bruta e capital fixo Capacidade empresarial Capacidade do conhecimento científico e tecnológico
Científica e tecnológica Recursos humanos, naturais e materiais e instituições C&T.	Educação e formação profissional Pesquisa e Desenvolvimento (P&D) Dinâmica produtiva Infraestrutura científica e tecnológica Inovação tecnológica
Psicossocial Escreve o ambiente cultural, religioso e étnico encontrado no TO/A Op. Descreve as crenças, valores, costumes e o comportamento dos membros da sociedade.	Cultura e padrões de comportamento Níveis de bem-estar Dinâmica estrutural

Tab B-1 – Expressões do poder militar

d. Gerenciamento do risco para as seguintes ameaças

- Nesse tópico devem ser listadas as ameaças críticas.

e. Meios recebidos e retirados

- Nesse tópico devem ser listados os meios recebidos e retirados.

2. MISSÃO DA SEGURANÇA DAS INFORMAÇÕES NAS OPERAÇÕES

- Retirado do enunciado da missão imposta, foco na **PROTEÇÃO** das Informações em operações.

- Deve ser a mais abrangente possível e não somente repetir a do escalão superior enquadrante.

3. EXECUÇÃO

- Expor, sinteticamente, para cada subgrupo de medidas da Segurança da Informação, as tarefas, com seus respectivos responsáveis, que serão implementadas para prevenir, obstruir, detectar, avaliar, explorar e neutralizar as ameaças com capacidade de colocar em risco as informações críticas. Deve ser aplicado em todos os escalões do combate.

a. Segurança da Informação nas Operações/Seg Org

- Apresentar as tarefas que deverão ser adotadas em cada um dos subgrupos de medidas de Segurança da Informação.

1) Segurança de Informação do Pessoal

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
Nr da IC	O que fazer.	Nível OM e/ou EM OM	Descrição completa	Nível do risco	Evitar, obstruir, detectar, avaliar, mitigar, eliminar e neutralizar.
IC 1 (exemplo)	Identificar e recrutar lideranças locais para influenciar a comunidade local	HUMINT das F Am do TO	Intlg da Ameaça recrutando Pop civil para obter Info Ctc	Alto	Prevenir/neutralizar o recrutamento de civis pela Intlg da ameaça.

2) Segurança de Informação da Documentação

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

3) Segurança de Informação do Material

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

4) Segurança de Informação das Áreas e Instalações

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
IC 2 (exemplo)	Empregar Armt para destruir o SARP	Tropa desdobrada no TO	IMINT emprega SARP para identificar local de tropa Bld	Alto	Detectar e neutralizar SARP da ameaça.

5) Segurança de Informação dos Meios de Tecnologia da Informação

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

b. Segurança Ativa

- Apresentar as tarefas que poderão ser adotadas em cada um dos Grupos de Medidas da Segurança Ativa, desconsiderando as que já foram previstas na Segurança Orgânica.

1) Contraespionagem

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

2) Contrassabotagem

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

3) Contraterrorismo

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

4) Desinformação

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

5) Contra-Ações Psicológicas

Cod Risco	Tarefas	Rspnl	Ameaça	Risco	Finalidade
					Rfr ¹

4. MEDIDAS ADOTADAS PARA A DESMOBILIZAÇÃO

- Apresentar as medidas de desmobilização (conforme Apêndice I).

5. PRESCRIÇÕES DIVERSAS

a. Para riscos quantificados como alto ou extremo, deverá ser confeccionada uma matriz de gerenciamento do risco, conforme preconizado no Cap VI deste Manual.

b. Prever, dependendo do Escalão, nivelamento de conhecimentos e treinamento das tropas, particularmente, as TTP para mitigar ou anular a ameaça à Seg Info Op.

APÊNDICE I AO ANEXO B

PLANO DE DESMOBILIZAÇÃO (Fundamentos)

1. PLANEJAMENTO ANTECIPADO

a. Plano de desmobilização: criar um plano detalhado que inclua etapas específicas para proteger informações críticas ou sensíveis.

b. Avaliação de riscos: identificar possíveis riscos de segurança da informação relacionados à desmobilização e estabelecer medidas de mitigação.

2. CONTROLE DE ACESSO E IDENTIFICAÇÃO

a. Revogação de acessos: garantir que todos os acessos a sistemas e informações críticas ou sensíveis sejam revogados imediatamente após a desmobilização.

b. Inventário de dispositivos: fazer um inventário de todos os dispositivos de comunicação e armazenamento (*laptops, tablets, smartphones* etc.) e garantir que sejam devolvidos ou devidamente protegidos.

3. SEGURANÇA DE COMUNICAÇÕES

a. Encerramento de comunicações: desativar ou redirecionar todos os canais de comunicação utilizados pela tropa, garantindo que nenhum acesso não autorizado ocorra.

b. Criptografia e destruição de dados: certificar-se de que todos os dados sensíveis sejam criptografados e, se necessário, destruir de forma segura os dados e dispositivos que não possam ser recuperados.

4. PROTEÇÃO DE DOCUMENTOS E MATERIAIS FÍSICOS

a. Coleta e destruição de documentos: recolher todos os documentos físicos contendo informações críticas ou sensíveis e garantir que sejam destruídos ou armazenados de forma segura.

b. Transporte seguro: implementar medidas de segurança para o transporte de documentos e equipamentos críticos ou sensíveis.

5. TREINAMENTO E CONSCIENTIZAÇÃO

a. Sessões de orientação: realizar sessões de orientação para as tropas sobre a importância da segurança da informação durante a desmobilização.

b. Boas práticas de segurança: reforçar as boas práticas de segurança como, por exemplo, não discutir informações críticas ou sensíveis em locais públicos ou não seguros.

6. MONITORAMENTO E AUDITORIA

a. Monitoramento contínuo: manter um monitoramento contínuo das atividades das tropas até que a desmobilização esteja completa para identificar e responder rapidamente a qualquer ameaça de segurança.

b. Auditoria pós-desmobilização: conduzir uma auditoria completa após a desmobilização para garantir que todas as medidas de segurança foram adequadamente implementadas.

7. GESTÃO DE INFORMAÇÕES E DADOS

a. Backup de dados: fazer *backups* de todas as informações críticas ou sensíveis antes da desmobilização e armazená-los em locais seguros.

b. Destruição de dados sensíveis: destruir de forma segura todos os dados críticos ou sensíveis que não são mais necessários.

8. COORDENAÇÃO COM AGÊNCIAS/ÓRGÃOS

a. Coordenação com inteligência e segurança: trabalhar em conjunto com órgãos de inteligência e segurança para monitorar e proteger informações durante a desmobilização.

b. Comunicação com aliados e parceiros: garantir que todas as informações compartilhadas sejam devidamente protegidas durante a desmobilização.

9. MANUTENÇÃO DE PROTOCOLOS DE SEGURANÇA

a. Continuidade dos protocolos de segurança: garantir que os protocolos de segurança continuem a ser seguidos até o final completo do processo de desmobilização.

b. Procedimentos de encerramento: implementar procedimentos claros para o encerramento seguro de operações e sistemas.

10.TECNOLOGIAS E FERRAMENTAS DE SEGURANÇA

a. Utilização de ferramentas de segurança: utilizar ferramentas de segurança cibernética, como *firewalls*, sistemas de detecção de intrusões e criptografia, para proteger informações durante o processo.

b. Atualização de sistemas: assegurar que todos os sistemas estejam atualizados com os últimos *patches* de segurança antes da desmobilização.

- Implantar essas medidas de forma integrada garantirá que a desmobilização das tropas ocorra de maneira segura, minimizando os riscos de comprometer informações sensíveis e assegurando a proteção contínua dos dados operacionais.

REFERÊNCIAS

BRASIL. Exército. Comando de Operações Terrestres. **Planejamento e Emprego da Inteligência Militar**. EB70-MC-70.307. 1. ed. Brasília, DF: COTER, 2016.

BRASIL. Exército. Comando de Operações Terrestres. **Companhia de Inteligência Militar**. EB70-MC-10.312. Edição Experimental. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Contraineligência**. EB70-MC-10.220. 1. ed. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Operações de Informação**. EB70-MC-10.213. 2. ed. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Produção do Conhecimento de Inteligência**. EB70-MT-10.401. 1. ed. Brasília, DF: COTER, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **Inteligência Cibernética**. EB70-MC-10.356. Edição Experimental. Brasília, DF: COTER, 2020.

BRASIL. Exército. Comando de Operações Terrestres. **Processo de Planejamento e Condução das Operações Terrestres**. EB70-MC-10.211. 2. ed. Brasília, DF: COTER, 2020.

BRASIL. Exército. Comando de Operações Terrestres. **Processo de Integração Terreno, Condições Meteorológicas, Inimigo e Considerações Cíveis – PITCIC**. EB10-MC-70.336. 1. ed. Brasília, DF: COTER, 2023.

BRASIL. Exército. Comando de Operações Terrestres. **Operações**. MC 3.0. 6. ed. Brasília, DF: COTER, 2025.

BRASIL. Exército. Estado-Maior do Exército. **Operações de Dissimulação**. EB20-MC-10.215. 1. ed. Brasília, DF: EME, 2014.

BRASIL. Exército. Estado-Maior do Exército. **Inteligência**. EB20-MC-10.207. 1. ed. Brasília, DF: EME, 2015.

BRASIL. Exército. Estado-Maior do Exército. **Inteligência Militar Terrestre**. EB20-MC-10.107. 2. ed. Brasília, DF: EME, 2015.

BRASIL. Exército. Estado-Maior do Exército. **Proteção**. EB20-MC-10.208. 1. ed. Brasília, DF, 2015.

BRASIL. Exército. Estado-Maior do Exército. **Glossário de Termos e Expressões para Uso no Exército**. EB20-MF-03.109. 5. ed. Brasília, DF: EME, 2018.

BRASIL. Exército. Estado-Maior do Exército. **Diretriz Reguladora da Política de Gestão de Riscos do Exército Brasileiro**. EB20-D-02.010. 1. ed. Brasília, DF: EME, 2019.

BRASIL. Exército. Estado-Maior do Exército. **Conceito Operacional do Exército – Operações de Convergência 2040**. EB20-MF-07.101. 1. ed. Brasília, DF: EME, 2023.

BRASIL. Exército. Estado-Maior do Exército. **Doutrina Militar Terrestre**. EB20-MF-10.102. 3. ed. Brasília, DF: EME, 2022.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Doutrina de Operações Conjuntas**. MD30-M-1. 2. ed. Brasília, DF: EMCFA, 2020. v. 1 e 2.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas**. MD33-M-02. 4. ed. Brasília, DF: MD, 2021.

COMANDO DE OPERAÇÕES TERRESTRES
CENTRO DE DOCTRINA DO EXÉRCITO
Brasília, DF, xx de xxxx de 2025
www.cdoutex.eb.mil.br